

FACTORS INFLUENCING THE ADOPTION OF  
BIOMETRIC SECURITY TECHNOLOGIES BY  
DECISION MAKING INFORMATION TECHNOLOGY AND SECURITY MANAGERS

by

David R. Lease

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

Capella University

October 2005

© David R. Lease, 2005

FACTORS INFLUENCING THE ADOPTION OF  
BIOMETRIC SECURITY TECHNOLOGIES BY  
DECISION MAKING INFORMATION TECHNOLOGY AND SECURITY MANAGERS

by

David R. Lease

has been approved

October 2005

APPROVED:

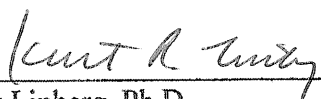
JEAN GORDON, D.B.A., Faculty Mentor and Chair

APIWAN BORN, Ph.D., Committee Member

RICHARD MURPHY, D.B.A., Committee Member

ACCEPTED AND SIGNED:

  
\_\_\_\_\_  
JEAN GORDON, D.B.A.

  
\_\_\_\_\_  
Kurt Linberg, Ph.D.  
Executive Director, School of Business

## Abstract

The research conducted under this study offers an understanding of the reasons why information technology (IT) and/or information assurance (IA) managers choose to recommend or not to recommend particular technologies, specifically biometric security, to their organizations. A review of the relevant literature provided the foundation to develop a set of research questions and factors for this research effort. The research questions became the basis of the study's stated hypotheses for examining managers' perceptions of the security effectiveness, need, reliability, and cost-effectiveness of biometrics. The research indicates that positive perceptions of security effectiveness, need, reliability, and cost-effectiveness correlate with IT/IA managers' willingness to recommend biometric security technologies. The implications of this study are that executives and managers can make informed decisions about the recommendation and adoption process relevant to biometric security technologies through an understanding of how perceptions of biometric technology affect the decision to recommend this type of technology. The study's results may also help biometric product developers, vendors, and marketers understand the important perceptions of biometric security technologies within their customer base of IT/IA managers.

## Dedication

This dissertation and entire doctoral work is dedicated to my supportive wife, Mahasti. Without her loving support – emotionally, physically, and spiritually – my doctoral work would have never progressed. She sacrificed greatly in many ways to allow me to work almost every night and weekend for over two years on my studies, research, and writing.

## Acknowledgments

My thanks and sincere appreciation goes to Dr. Jean Gordon, the finest teacher and mentor I could possibly want. Dr. Gordon provided continuous encouragement, strategic thinking, goal focus, and sincere friendship throughout my program. She redefines mentor, and I am truly fortunate to have developed a lifelong friend and colleague in her. My hope is that I will be able to honor her by giving to another student the level of friendship, trustworthiness, and guidance that she gave to me.

I would also like to acknowledge and thank my other very important committee members: Dr. Apiwan Born and Dr. Dick Murphy. As a teacher and committee member, Dr. Born challenged me to look beyond my research, to evaluate critically my sources, and to develop my own research “voice” in my studies. Dr. Murphy provided extraordinary encouragement and support throughout the dissertation process. I could not have accomplished my research and dissertation without their genuine concern, motivation, and intellectual challenges.

## Table of Contents

Acknowledgments	v
List of Tables	ix
List of Figures	xi
CHAPTER 1. INTRODUCTION	1
Introduction to the Problem	1
Background of the Study	2
Statement of the Problem	3
Purpose of the Study	3
Rationale for the Study	4
Research Questions	5
Research Hypotheses	7
Significance of the Study	7
Definition of Terms	8
Assumptions and Limitations	10
CHAPTER 2. LITERATURE REVIEW	11
Introduction and Organization	11
Section 1: Biometric Authentication Controls: Purpose and Problems	13
The Importance of Identification and Verification	14
Biometric Technologies as a Potential Security Solution	18
Biometric Technologies: Fundamentals, Types, and Major Issues	23

Types of Biometric Technologies	30
Disadvantages and Problems with Biometric Technologies	47
Biometrics in Action	60
Advantages and Disadvantages of the Various Biometric Technologies	63
Summary and Recommendations for Considering Biometrics	66
Gaps in the Literature Regarding Biometrics	67
Section 2: Organizational Decision Making Overview	67
Gaps in the Literature Regarding Decision.Making	73
CHAPTER 3. METHODOLOGY	76
Theoretical Framework	76
Research Questions	77
Research Hypotheses	77
Sample Design	79
Variables	80
Field/Pilot Trials	84
Validity and Reliability	85
Minimum Sample Size Determination	90
Survey Instrument	92
Data Collection	92
Data Confidentiality	98
Data Analysis	99



Potential Limitations of the Study Methodology	103
CHAPTER 4. DATA COLLECTION AND ANALYSIS	105
Data Collection, Response Rates, and Population	105
Demographic Characteristics of the Sample	106
Descriptive Statistics	118
Exploratory Factor Analysis	119
Hypothesis Testing	128
Summary of Data Collection and Analysis	134
CHAPTER 5. STUDY RESULTS, CONCLUSIONS, AND RECOMMENDATIONS	136
Hypotheses	139
Study Design	141
Discussion of the Findings	143
Implications of the Study	145
Suggestions for Further Research	146
Conclusions	151
REFERENCES	154

## List of Tables

Table 1. Comparative Market Share of Biometric Technologies	31
Table 2. Accuracy/Error Rates of Leading Biometric Technologies	46
Table 3a. Comparison of Leading Biometric Technologies	64
Table 3b. Comparison of Leading Biometric Technologies	65
Table 4. Research Hypotheses	78
Table 5. Pearson's <i>r</i> Correlation Coefficients	88
Table 6. Kendall's <i>tau b</i> Correlation Coefficients	88
Table 7. Spearman's <i>rho</i> Correlation Coefficients	89
Table 8. Comparison of Changed Responses	90
Table 9. Data Collection and Analysis Summary	99
Table 10. Previous Experience Frequency Distribution	107
Table 11. Previous Experience and Recommendation Crosstabulation	109
Table 12. Organization Size Frequency Distribution	109
Table 13. Organization Size and Recommendation Crosstabulation	111
Table 14. Title/Job Function Frequency Distribution	112
Table 15. Title/Job Function and Recommendation Crosstabulation	114
Table 16. Industry Frequency Distribution	115
Table 17. Industry and Recommendation Corsstabulation	117
Table 18. Means and Standard Deviations	118
Table 19. Inter-Item Correlation Matrix	119

Table 20. Selection of the Number of Factors to Retain	121
Table 21. Total Variance Explained	122
Table 22. Component Correlation Matrix	122
Table 23a. Rotated Component Pattern Matrix	123
Table 23b. Rotated Component Pattern Matrix	124
Table 24. Rotated Component Structure Matrix	125
Table 25. Final Component Loadings	127
Table 26. Hypothesis Testing: Correlation Analysis	128
Table 27. Crosstabulation for Hypothesis 1	129
Table 28. Chi Square Tests for Hypothesis 1	129
Table 29. Crosstabulation for Hypothesis 2	130
Table 30. Chi Square Tests for Hypothesis 2	131
Table 31. Crosstabulation for Hypothesis 3	132
Table 32. Chi Square Tests for Hypothesis 3	132
Table 33. Crosstabulation for Hypothesis 4	133
Table 34. Chi Square Tests for Hypothesis 4	134

## List of Figures

Figure 1. Test–retest scatterplot	87
Figure 2a. Biometrics data collection instrument	95
Figure 2b. Biometrics data collection instrument	96
Figure 3a. Demographics data collection instrument	97
Figure 3b. Demographics data collection instrument	98
Figure 4a. Biometrics question coding protocol	100
Figure 4b. Biometrics question coding protocol	101
Figure 5a. Demographic information coding protocol	101
Figure 5b. Demographic information coding protocol	102
Figure 6. Distribution of previous experience	108
Figure 7. Distribution of organization size	110
Figure 8. Distribution of title/job function	113
Figure 9. Distribution of industries	116

## CHAPTER 1. INTRODUCTION

### Introduction to the Problem

Information security technologies continually evolve to meet new security threats. As a reflection of the increased need to protect organizations' information from both internal and external threats, many organizations have begun investigating the adoption of biometric security technologies as a significant component in their overall security architecture. An example of the astounding growth in this market, the International Biometric Group (IBG) expects biometrics industry revenue to increase from under \$50 million in 2004 to almost \$200 million in 2008 (Reynolds, 2004). Understandably, a wealth of information exists regarding biometric technologies and the technical trade-offs in implementing biometric solutions. Notwithstanding a substantial body of literature on the technical aspects of biometric security technologies, little scholarly research has been undertaken regarding the critical factors that influence decision makers when they recommend that biometrics be adopted in their organizations. This dearth of scholarly research may be a reflection of the relative immaturity of the biometrics market. Further, trade magazines differ widely in their surveys of managers and/or their perceptions of information technology security and leave little in the way of data to aid management in making a solid security technology choice for their organization.

The researcher conducted primary research in order to evaluate information technology (IT) and/or information assurance (IA) managers' attitudes and perceptions of the security effectiveness, need, reliability, and cost-effectiveness of biometric authentication

controls and to identify the association of their attitudes and perceptions to their willingness to recommend biometric security technologies.

### Background of the Study

Biometric security technology has complex characteristics that often make the process of organizational adoption decisions difficult. Perceptions of a specific security technology, its effectiveness, reliability, and the need for the technology and its cost-effectiveness are important elements in the decision to recommend the technology to an organization (Craig & Hamidi-Noori, 1985; Etlie, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004). Additionally, organizations are increasingly attentive to the cost of security and demand that IT security expenditures be proportionate to IT security risks (Center for Digital Strategies, 2005; Lanzi, 2002; Lawlor, 2005; Lesk, 2003; Levine, 2004; Richards, 2002; Shore, 2004; Verton, 2003). However, many if not most, major investments are subject to some form of cost-benefit and/or return-on-investment analysis. This practice has been less common in IT investments in general and in IT security investments in particular because of inherent difficulties in applying traditional ROI analysis to IT and because of a lack of clear models (Au & Kauffman, 2002; Mercuri, 2003; Nguyen, 2004; Orlandi, 1991; Soo Hoo, 2000). This study sought to shed light on this process in order to help decision makers, as well as biometric product developers and vendors, understand the important perceptions of biometric security technologies within their customer base of IT/IA managers.

### Statement of the Problem

Determining if a particular technology is appropriate often can be a guessing game based on word-of-mouth, vendor and consultant recommendations, and trade magazine reviews. Repeatedly, managers and executives are left guessing about what security technologies will be used in the future and whether or not IT/IA professionals consider one technology more secure, necessary, reliable, or cost-effective than another technology. This uncertainty can lead to poor decision making, costly mistakes, and unmitigated security vulnerabilities.

Dynes, Brechbuhl, and Johnson (2005) explored the main drivers of private sector organizational adoption of IT security through a field study of a Fortune 500 manufacturing firm and four of its direct suppliers. They found that the primary driver of the firm's selection and adoption of information security was the IT security manager's recommendations on how best to protect their firm's IT assets. Based on the findings in this research, this study focused on the factors that influence IT security managers to recommend biometric security technologies. Drawing from the extant literature and further refinement of the relevant concepts, the study gauged the influence of security effectiveness, need, reliability, and cost-effectiveness on managers' decisions to recommend biometric security technologies.

### Purpose of the Study

The general purpose of this study was to help IT/IA decision makers select appropriate security solutions for their organizations by focusing on the critical factors contributing to the decision to recommend new technologies. The specific purpose was to

investigate the factors that influence IT/IA managers to recommend biometric security technologies. The study will also provide security technology companies with information to assist them in the determination of what is important to their customer base when considering the introduction of new IT security products.

### Rationale for the Study

Researchers who have examined the problem of new IT adoption have drawn extensively from theories developed in innovation adoption and in social psychology with a number of models proposed to guide inquiry into this phenomenon (Agarwal & Prasad, 2000, 1998; Ajzen, 1988; Brancheau & Wetherbe, 1990; Davis, 1989; Kwon & Zmud, 1987; Rogers, 2003). Despite the existence of these models and the many divergences in hypothesized associations, a common theme underlying these models is the inclusion of perceptions of a new technology as independent variables. Everett M. Rogers' (2003) model of the diffusion of innovations portrays attitudes toward a new technology as antecedents to the decision to adopt the new technology. Fred Davis's (1989) technology acceptance model and its precursor, the theory of reasoned action (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975), both postulate that attitudes or perceptions about a technology are instrumental in the decision to adopt the technology.

Recent research (Dynes, Brechbuhl, & Johnson, 2005) has indicated that IT/IA managers' recommendations of IT security products and technologies were the primary drivers for organizational adoption of security technologies. The important role played by



perceptions of a technology as well as the pivotal role of IT/IA managers in the security technology adoption decision process clearly highlights the need for research in this area.

Further, a number of researchers have ascribed to the rationale for the choice to recommend a new technology to perceptions of its cost-effectiveness, reliability, organizational need, and function-effectiveness (Craig & Hamidi-Noori, 1985; Ettl, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004). Drawing from the work of these researchers and through further development of the relevant concepts, a series of research questions and hypotheses was developed.

This study helps executives and managers make informed decisions about the recommendation and adoption process relevant to biometric security technologies by evaluating IT/IA managers' perceptions of cost-effectiveness, reliability, organizational need, and security (function)-effectiveness. The IT/IA managers' attitudes can provide real-life clues into the perceived usefulness of biometric technology and can be a significant factor in the decision to recommend this type of technology.

### Research Questions

Organizational decision making can be quite complicated when considering the adoption of a new technology. Biometric security technology has capabilities, features, and challenges that compound the difficulty of making the decision to recommend the technology. The overall goal of this research was to give organizational decision makers improved insight and knowledge into making often difficult and complex decisions about security technology adoption.

Recent research has indicated that the perceptions of IT/IA managers and professionals are predominant factors in organizational decision making regarding the adoption of security technology (Dynes, Brechbuhl, & Johnson, 2005). Based on these findings, it is appropriate to evaluate the perceptions of IT/IA managers regarding biometric security technologies and their willingness to recommend or not to recommend biometrics as integral elements in the overall organizational technology adoption decision process. With regard to the evaluation of specific perceptions of technologies, a number of researchers have ascribed the rationale for the choice to recommend a new technology to perceptions of its cost-effectiveness, reliability, organizational need, and function-effectiveness (Craig & Hamidi-Noori, 1985; Ettl, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004).

Drawn from the extant literature and with further development of the relevant concepts, this study investigated the following four research questions. Each of the research questions gauges the respective aspects of IT/IA managers' perceptions of biometrics relative to the following factors identified in the literature: security effectiveness, need, reliability, and cost-effectiveness of biometrics. The specific research questions were as follows:

Question 1: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its security effectiveness?

Question 2: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perceived need for new security technologies?

Question 3: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its reliability?

Question 4: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its cost-effectiveness?

### Research Hypotheses

Based upon the above research questions, the study tested the following hypotheses:

Hypothesis 1: An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its security effectiveness.

Hypothesis 2: An IT/IA manager's decision to recommend biometric security technology is independent of his/her perceived need for new security technologies.

Hypothesis 3: An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its reliability.

Hypothesis 4: An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its cost-effectiveness.

### Significance of the Study

This study significantly contributes to the data in the fields of information technology and information assurance (security). It added new knowledge in these fields and highlighted the importance of the perceptions of IT/IA managers regarding biometric security technologies. It helped determine business reasons for IT/IA managers' recommendations to adopt biometric technology. It also presented insight into why IT/IA professionals may recommend one biometric security technology over another and offered some areas for consideration to organizations contemplating the use of biometric security technology. Additionally, the study provided security technology companies and developers of information security products with information to assist in the determination of what is important to their customer base when considering the introduction of new IT security products. In the future, business and technology managers will be interested in this data when contemplating the adoption of biometric security technologies.

### Definition of Terms

*Biometrics.* Biometrics is “the automatic identification of a person based on his or her physiological or behavioral characteristics” (Chirillo & Blaul, 2003, p. 2). Biometrics is generally used as a noun to refer to the automatic recognition of individuals based on their physical and/or behavioral characteristics. The term, biometric, can be used as a noun in reference to a single technology or measure (e.g., finger scan is a commonly used biometric) or as an adjective as in “a biometric system uses integrated hardware and software to conduct identification or verification” (Nanavati, Thieme, & Nanavati, 2002, p. 11).

*Crossover Error Rate.* The crossover error rate (CER) – also known as the Equal Error Rate (EER) – is a comparison metric for different biometric devices and technologies. The CER is the point at which the false acceptance rate equals the false rejection rate. In general, a lower CER indicates higher reliability and accuracy (Liu & Silverman, 2001).

*Enrollment.* Enrollment is the initial process of collecting biometric data from a user and then storing it in a template for later comparison (Liu & Silverman, 2001).

*Failure to Enroll.* Failure to enroll (FTE) is when “an individual is unable to enroll [his/her] biometric in order to create a template of suitable quality for subsequent automated operation” (Ashbourn, 2004, p. 10). Common reasons for failure to enroll include physical disability and a user whose physiological/behavioral characteristics are less distinctive than average (Ashbourn, 2004).

*False Acceptance Rate.* The false acceptance rate (FAR) is the measure of imposters incorrectly matched to a valid user’s identity. FAR is expressed as a percentage (Liu & Silverman, 2001).

*False Rejection Rate.* The false rejection rate (FRR) is the measure of incorrectly rejected valid users. FRR is expressed as a percentage (Liu & Silverman, 2001).

*Identification.* Identification is the process by which the biometric system verifies a person by performing a one-to-many search against the entire enrolled population (Liu & Silverman, 2001).

*Information Technology.* Information technology is the “technology required for information processing. In particular, the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information from anywhere, anytime” (Wikipedia, 2005, n.p.).

*Information Assurance.* Information assurance pertains to the operations that “protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This protection and defense includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities” (ATIS, 2005, n.p.).

*Template.* A template is a mathematical representation of biometric data. It can vary in size from nine bytes for hand geometry to several thousand bytes for facial recognition (Liu & Silverman, 2001). Templates “are not raw data or the scanned images of a biometric sample, but rather they are an accumulation of the distinctive features extracted by the biometric system” (Woodward, Orleans, & Higgins, 2003, p. 37).

*Verification.* Verification is the authentication process by which the biometric system matches a captured biometric against the individual’s stored template (Liu & Silverman, 2001, p. 29).

### Assumptions and Limitations

The survey was limited specifically to IT and IA professionals in a management role. Management role was defined by the individual's title in the organization and was not dependent on an explicitly defined supervisory role. The study was also limited specifically to biometric security technologies and did not include other security technologies, except to draw comparisons and contrast responses in the survey.

An assumption was made that the sample of IT/IA managers is representative of IT/IA managers in the Mid-Atlantic (Maryland, Virginia, and the District of Columbia) area of the U.S. regarding their attitudes about biometric security technologies. Randomness of the target sample was preserved because each member of the sample had an equal opportunity to complete the survey.

Fowler (1993) has argued that non-response is a potential source of bias in voluntary studies. For this study, non-response was addressed by comparing the responses of early responders to those of late responders. Although not investigated, the day of the week and/or time of day may have introduced some bias into responses to the survey. Additionally, because all answers were kept confidential with personal identification information deleted, the researcher assumed the respondents answered honestly because there would be no fear of reprisal.

## CHAPTER 2. LITERATURE REVIEW

### Introduction and Organization

The purpose of this study was to help information technology (IT) and/or information assurance (IA) decision makers select appropriate security solutions for their organizations by focusing on the critical factors that influence IT/IA managers to recommend biometric security technologies. Specifically, the research can help information technology management professionals determine if the security effectiveness, organizational need, reliability, and cost/value aspects of biometric security technologies are generally acceptable to IT/IA decision makers. The study may also provide security technology companies with information to assist in the determination of what is important to their customer base when considering the introduction of new IT security products.

The literature review in this chapter presents an overview and analysis of the two fundamental topics underlying this research effort: biometric security technologies and the decision processes relevant to a manager's decision to recommend or not to recommend a new technology. The first section of the literature review provides an overview of biometric security technologies commonly used in contemporary business operations. This overview provides a comprehensive framework for understanding the importance of studying biometric security technologies and their use in industry and for understanding the many factors that impact IT/IA managers' decision to recommend biometrics. The review presents an analytical and comparative study of biometric authentication methods commonly used in contemporary business operations with a focus on the five most widely deployed biometric technologies – fingerprint verification, facial recognition, hand geometry verification, iris

recognition, and voice verification. The first four biometric technologies are based on recognition/verification of a physiological characteristic of a person, but the last one involves verification of a behavioral characteristic, particularly the voice.

The overview of biometric security technologies is organized into four main sections. Part 1 provides an overview of the current state of authentication controls in most business operations, considers the reasons why organizations need improved controls, and looks at how the implementation of biometrics might fill that need. In this section, factors encouraging and discouraging the business application of biometrics are identified. Part 2 explains the basics of biometric technology and presents a comparative analysis of leading biometrics. This part also explores the reasons for organizations' reluctance to adopt biometrics, in particular, user objections regarding privacy concerns and the ethical issues involved in biometrics implementation. In an effort to understand the promises, limitations, and possible business applications of biometrics, Part 3 examines the actual experiences that organizations, public institutions, and government agencies have with biometrics implementation. The concluding section of the overview of biometric security technologies provides a summary of the research from the perspective of business-based applications. This summary is followed by recommendations designed to assist organizations in making decisions about biometrics adoption and in implementing biometric authentication and identification controls. The concluding section also discusses a gap in the literature in which further research into the factors influencing the decision to implement biometric security technologies would be useful and appropriate.



The second section of the literature review discusses the concepts of technology decision making processes, organizational decision making units, and the influences of attitudes and perceptions on decision making in light of the related organizational decision making literature. Additionally, from the review of the pertinent literature, various factors that influence the technological decision processes in organizations are identified. The concepts derived from the extant literature are further elaborated to formulate the research questions investigated in this study. These decision factors and research questions form the basis for the hypotheses that were tested for this study.

#### Section 1: Biometric Authentication Controls: Purpose and Problems

Once exclusively the purview of law enforcement, intelligence, and national security agencies, biometrics – the automated recognition of people based on their physiological and/or behavioral characteristics – now promises to emerge into the business mainstream as a method of identification and authentication for access to physical and logical infrastructure (Ashbourn, 2004; Boroshok, 2005a, 2005b; Ferraro, 2003; Jain, 2004). Biometric authentication technologies promise substantially improved security, convenience, and portability over other commonly used methods of authentication (Ashbourn, 2004; Chirillo & Blaul, 2003; O’Gorman, 2003). Falling costs, improvements in technologies, increased security needs, and changing government regulations also encourage the adoption of biometrics. Notwithstanding these factors, few firms to date have implemented biometric authentication controls (Grimes, 2003; Hurley, 2003; Vijayan, 2004).

### The Importance of Identification and Verification

Ensuring the identity and authenticity of persons is a prerequisite to security and efficiency in modern business operations. Unauthorized intruders can damage physical and logical infrastructure, steal proprietary information, compromise competitiveness, and threaten business sustainability. Traditional methods of recognition and identification, wherein one individual identifies another based on his or her voice, physical appearance, or gait, are impractical, inefficient, and potentially highly inaccurate in the scope of contemporary business operations. To address the need for rapid, efficient, and cost-effective authentication, organizations today primarily rely on the two methods of “what you have” and “what you know” (either applied individually or in combination) to verify the identity of persons accessing their physical and/or logical infrastructure.

#### *What You Have*

To verify the identity of authorized users (e.g., employees, suppliers, customers, etc.) under the what you have method, users present certain tangible possessions such as ID badges, Smart Cards, or keys to gain access to the physical and/or logical infrastructure. In this case, users are authenticated based on something in only their possession and, theoretically, not available to other people.

#### *What You Know*

The what you know method requires that authorized users present certain bits of information such as passwords, pass phrases, personal identification numbers (PINs), or code answers to gain access to the physical and/or logical infrastructure. In this case, users are authenticated based on something that (again theoretically) only the authorized user knows

(Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Liu & Silverman, 2001; Matyas & Riha, 2003; Nanavati, Thieme, & Nanavati, 2002; O’Gorman, 2003; Zhang, 2002).

From both security and practical perspectives, these methods of authentication are problematical (Ashbourn, 2004; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Nanavati, Thieme, & Nanavati, 2002; O’Gorman, 2003). Identification methods that are based on what one possesses are advantageous in that they are highly visible, portable, and do not require the user to remember complex passwords or multiple user ID/password combinations. On the other hand, keys, badges and the like can be lost, stolen, duplicated, destroyed, shared, or forgotten. Moreover, this latter method does not directly authenticate the user (Chandra & Calderon, 2003). Unauthorized users and imposters will be falsely recognized as authorized users based on their possession of a legitimate key, token, badge, or other authorized possession.

Intuitively, verifying identity based on what a person knows would appear to provide a much higher level of security than verification based on what one has. Like the ID badge or Smart Card, the user ID/password provides an unambiguous basis for identity verification. The password is either valid or invalid. A password that is close to the valid password will not provide entry. The relative lack of visibility of the PIN/password when compared to the ID badge and other possession-based means of identification provides an advantage in that it is less obviously vulnerable to theft.

A closer examination of this method of authentication, however, revealed multiple problems and vulnerabilities (Anderson, 2001; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chandra & Calderon, 2003; Ferraro, 2003; Higbie, 2004; Liu & Silverman, 2001;

O’Gorman, 2003; Schneier, 1999; Strassmann, 2002). The user ID/password/PIN method of authentication is relatively robust and secure as long as it operates in practice as it is supposed to in theory. Ideally, the user develops a unique user ID and password for *each* required point of access. The password should be devised in a way that would make it difficult for anyone to guess correctly. The password should be kept secret, not written down or shared, and held safely in the memory of the user. Finally, the user must be able to recall quickly and accurately the correct user ID/password combination for each access situation. Unfortunately, in practice, users often fail to develop unique passwords for each required point of access, opting instead to reuse the same password for multiple applications. In practice, users also often fail to develop demonstrably unique and hard-to-guess passwords. Instead, they frequently choose the names of their children, birth dates, names of pets, and other easy-to-remember (and guess) passwords. Although ideally users should commit their passwords to memory, many users find the need to write down their passwords, sometimes in obvious places such as under “P” in their address books. All of these factors make it more likely that an unauthorized user can successfully guess and/or steal a password and gain access to confidential information. Further breaches of security can occur when users voluntarily share their user ID/passwords with friends and coworkers. Thus, as is the case with authentication based on possession, authentication based on what one knows does not directly authenticate the user (Chandra & Calderon, 2003; O’Gorman, 2003).

Another, and perhaps the most critical, shortcoming with the reliance on the password, or some variation thereof, method of authentication is that it requires reliance on human memory. As Help Desk/technical support centers around the world have attested,

users routinely and regularly forget their passwords, including forgetting where they wrote them, resulting in excess expenditures for password resets and system maintenance (Ammenheuser, 2002; O’Gorman, 2003; Saccomano, 2003; Strassmann, 2002; Zhang, 2002). The password problem has grown dramatically and promises to worsen significantly in the future as a result of the growing complexity of business operations and the expansion of information and communication networks with multiple points of access that require users to create and remember dozens or even hundreds of different complex user ID/password combinations (Anderson, 2001; Ashbourn, 2004; Chirillo & Blaul, 2003; Hill, 2001; Nanavati, Thieme, & Nanavati, 2002; Schneier, 1999; Woodward, Orleans, & Higgins, 2003; Zhang, 2002). Smart Cards and Universal Serial Bus (USB) keys capable of storing multiple passwords along with other key identity information are sometimes offered as a solution to the password problem, but, as previously noted, these possession-based authentication systems have their own set of problems and vulnerabilities.

Coupled with the denigration of security robustness in commonly used what you have and/or what you know authentication systems, there has been an *increase* in business security threats. The widespread move to wireless and portable information systems has not only led to increased convenience and efficiencies but also exposed new vulnerabilities (“Authentication Questions and Answers,” 2002; Higbie, 2004; Hwang & Verbauwhede, 2004; Strassmann, 2002). Additionally, these increased threats have occurred at a time when information system security threats from hackers, thieves, and others have multiplied dramatically (Anderson, 2001; Nanavati, Thieme, & Nanavati, 2002; O’Gorman, 2003; Zhang, 2002). Moreover, the September 11, 2001, terrorist attacks raised the very real

possibility of a terrorist attack not only against commercial physical infrastructures (e.g., office buildings, manufacturing plants, aircraft, etc.) but also, perhaps even more critically, against commercial and government information infrastructures (e.g., networks, servers, databases, etc.) (Boroshok, 2005a; Ledford, 2002; Markowitz, 2002; McHale, 2003; Scheier, 2002; Woodward, Orlans, & Higgins, 2003). Therefore, in a security-focused environment, organizations are increasingly concerned about ways to ensure that the people who access their physical infrastructure and their information/communication networks are in fact the people who they have authorized to do so.

### Biometric Technologies as a Potential Security Solution

Biometrics have long been touted as a possible solution to the problems and vulnerabilities of other commonly used methods of authentication and identification. They represent sophisticated versions of the traditional means of identification, such as a guard allowing access to a user whom he/she recognizes by sight. Biometrics are commonly defined as automated methods of recognition/verification/identification of individuals based on some measurable physiological or behavioral characteristics such as fingerprints, hand geometry, facial shape, iris pattern, voice, signature and the like (Ashbourn, 2004; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chirillo & Blaul, 2003; Jain, 2004; Matyas & Riha, 2003; Nanavati, Thieme, & Nanavati, 2002). Whereas ID badges and keys authenticate the user based on something the user possesses, and passwords/PINs authenticate the user based on what the user knows, biometrics allows authentication and identity verification based on who the user *is*. Because biometric methodologies of authentication actually base

identification on physiological or behavioral “pieces” of the user, biometrics represents the only form of authentication that *directly authenticates the user* (Chandra & Calderon, 2003; Jain, 2004; Nanavati, Thieme, & Nanavati, 2002; Woodward, Orlans, & Higgins, 2003).

Biometrics have a number of other obvious advantages over other commonly used authentication methods (Ashbourn, 2004; Chandra & Calderon, 2003; Chirillo & Blaul, 2003; Harris & Yen, 2002; O’Gorman, 2004; Prabhakar, Pankanti, & Jain, 2003). Unlike an ID badge or a USB key, one cannot easily lose or misplace a fingerprint or other biometric measures. Likewise, unlike the case with passwords and PINs, one does not need to remember and one is not subject to forgetting a physiological or behavioral characteristic.

While biometric measures *can* be compromised, in general, a biometric is much more difficult to manipulate by stealing, forging, sharing, or destroying than other commonly used authentication tools. Biometrics also provide considerable convenience, as opposed to the hassle of memorizing dozens of passwords. Because biometric identifiers are not easily lost or compromised and because they are not dependent upon fallible human memories, the implementation of biometric systems typically results in much lower administrative costs (i.e., fewer calls to the Help Desk for technical support to reset passwords, no need to issue replacement ID badges, etc.) than other access methodologies. For these and other reasons, biometrics are viewed as providing better security, increased efficiency, and more reliable identity assurance than other commonly used methods of authentication/identification based on what a user possesses or what a user knows.

Biometric methods of identification and identity verification, including automatic fingerprint analysis and facial recognition technologies, have been available and used by

some government/public agencies (e.g., law enforcement, intelligence, and national security) and a few private industries (e.g., facial recognition scans in casinos) since the 1960s and 1970s (Chirillo & Blaul, 2003; Woodward, Orlans, & Higgins, 2003). Notwithstanding its potential benefits and multiple advantages over other authentication methods, biometrics have not been widely applied, particularly in the corporate world. Analysts cite high costs of equipment and implementation, technological problems, vulnerabilities of specific biometrics, lack of standards, and user resistance (notably, concerns over privacy) as reasons for the lack of implementation (Alterman, 2003; Ashbourn, 2004; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chirillo & Blaul, 2003; Glass, 2004; Hamilton, 2003; Nanavati, Thieme, & Nanavati, 2002; Rupley, 2002; Prabhakar, Pankanti, & Jain, 2003; Woodward, Orlans, & Higgins, 2003).

However, over the past few years significant improvements in biometric technologies, a movement towards standardization, changes in regulations requiring organizations to adopt stringent security and privacy controls, and significantly reduced costs have encouraged widespread adoption. A number of government agencies (e.g., Department of Homeland Security, Department of Transportation, Department of Defense, Customs and Border Protection, Department of Justice, National Library of Medicine) and businesses in certain industries (e.g., healthcare and finance) have significantly increased their use of biometrics during the past few years – a factor that is likely to encourage other organizations to adopt biometrics as well (McHale, 2003; “Prepare to be Scanned,” 2003; Reynolds, 2004; Ward, 2004). At least one major computer manufacturer has banked on these rapid developments in biometrics applications. In late 2004, IBM became the first major computer manufacturer to



add biometric components to its computers (“Biometrics, Trusted Computing Key,” 2004; Van, 2004). IBM announced that it would be adding fingerprint scanners on all of its ThinkPad® notebook computers, enabling users to increase security by requiring a finger swipe and a password (or just a finger swipe) to access files. IBM indicated that it eventually planned on adding biometric authentication controls to all of its other mobile devices and to its desktop computer keyboards. Most analysts see the September 11 terrorists’ attacks also as a key impetus behind the increased usage of biometrics for authentication and identification. The terrorist attacks have been critical in encouraging adoption not only because they have heightened companies’ and agencies’ security concerns but also because the impact and implications of the terrorists’ attacks seem to have lowered users’ resistance to the use of biometrics by employers and government (Boroshok, 2005a; Chirillo & Blaul, 2003; Ferraro, 2003; McHale, 2003; Pallay, 2003; Schneier, 2005; Woodward, Orleans, & Higgins, 2003). In other words, in the same way as the September 11 attacks reduced public objections to possible infringements on civil liberties as a result of implementation of Public Law No. 107-56, the USA PATRIOT Act, and other security-focused measures, these attacks also appear to have rendered many people less sensitive to the potential privacy-invading implications of biometrics. Boroshok (2005a) reported that a recent survey sponsored by AuthenTec found that 71% of U.S. consumers would pay more for biometric security options in their cell phones and 63% of consumers would pay an additional cost for these options to be added to their personal computers.

The changing security environment has prompted expectant forecasts of rapid growth in biometrics. In a December 2001 report, market research firm IDC predicted that

worldwide biometrics spending would rise at a 50% compounded annual growth rate from \$119 million in 2000 (Scheier, 2002). In 2004, the International Biometric Group (IBG) predicted rapid growth for the biometrics industry over the next several years from revenues totaling under \$50 million in 2004 to revenues of almost \$200 million in 2008 (Reynolds, 2004). In late 2003, analysts at the San Jose, California-based market research firm Frost and Sullivan predicted that biometric applications from commercial applications (not including the government's Automated Fingerprint Identification System or AFIS) would jump from \$93.4 million in 2001 to \$2.05 billion by 2006 – up from the \$700 million (in 2006) that these analysts predicted prior to the September 11, 2001 attacks (McHale, 2003).

Despite the many forces favoring business implementation of biometrics and notwithstanding industry analysts' enthusiastic projections, businesses, for the most part (companies in the financial and healthcare industry stand out as notable exceptions), have been hesitant to embrace biometrics (Boroshok, 2005b; Hulme, 2003; Vijayan, 2004). Some firms continue to cite cost issues and privacy concerns, while others point to problems surrounding biometric implementation in airports and among government agencies ("Biometrics Not Yet Ready to Secure Corporate IT," 2004; Glass, 2004; Hulme, 2003; Vijayan, 2004). Overall, surveys of companies indicate that forecasts of dramatic and rapid growth in biometrics implementation may be overstated. Hulme (2003) reported that "only 9% of 300 business-technology executives surveyed for the *InformationWeek* Research Priorities 1Q2003 study say biometric deployment is a key business priority, down from 12% in the same quarter of 2002" (p. 57). A 2003 Forrester Research survey found that only 1% of companies had implemented biometric systems, just 3% had a biometric system rollout in

progress, only 15% were testing biometrics, and 58% of those surveyed had *no plans* to try biometrics (Hulme, 2003).

## Biometric Technologies: Fundamentals, Types, and Major Issues

### *Overview of Biometric Technologies and Biometric Systems*

*History and definition.* The use of non-automated biometrics dates back to the beginning of human civilization, when individuals first began identifying other individuals based on certain physical or behavioral characteristics. Woodward, Orleans, and Higgins (2003) noted that the concept of biometrics as an organized system of authentication dates back to more than one thousand years in East Asia, when potters placed their fingerprints on their wares as an early form of brand identity. Anderson (2001) cites the use of handwritten signatures (chops) in classical China as an example of an early biometric. The development of contemporary biometric systems can be viewed as an outgrowth of the efforts of forensic scientists and law enforcement agencies to identify and classify criminals in the late 19<sup>th</sup> and early 20<sup>th</sup> centuries. Fully automated biometric systems, including AFIS used by law enforcement agencies and commercial biometric systems (typically relying on hand geometry) designed for use in physical access to buildings, emerged in the 1960s and 1970s.

The contemporary meaning of biometrics emphasizes its automated aspects, which allow for deployment on a large scale. As previously noted, the most widely cited definition of biometrics is some variation of “the automatic identification of a person based on his or her physiological or behavioral characteristics” (Chirillo & Blaul, 2003, p. 2). The term *biometrics* is generally used as a noun to refer to the automatic recognition of persons based

on their physical and/or behavioral characteristics. The term *biometric* can be used as a noun in reference to a single technology or measure (e.g., finger scan is a commonly used biometric) or as an adjective as in “a biometric system uses integrated hardware and software to conduct identification or verification” (Nanavati, Thieme, & Nanavati, 2002, p. 11).

#### *Properties of biometrics*

Biometrics are based on the measurement and matching of distinctive physiological and/or behavioral characteristics. The former are based on direct measurement of a physiological characteristic of some part of the human body. Examples of physiological biometrics include finger, hand, retina, and iris scans. On the other hand, the latter *indirectly* measure characteristics of the human body based on measurements and data derived from an action (Nanavati, Thieme, & Nanavati, 2002). Commonly used behavioral biometrics include voice and signature scan and keystroke pattern.

In theory, almost any human physiological and/or behavioral characteristic can be used as a biometric measure. However, to fit within a viable, potentially accurate, and practical biometric system, the biometric used should also satisfy four other requirements offered by Jain (2004) and Bolle, Connell, Pankanti, Ratha, and Senior (2004):

1. Universality: Every person should have the biometric characteristic
2. Uniqueness: No two persons should be the same in terms of the biometric characteristic. Jain (2004) proposed the somewhat lower standard of distinctiveness, defined as “any two persons would be sufficiently different in terms of the characteristic” (p. 3)
3. Permanence: The biometric should be relatively invariant over a significant period

of time

4. Collectability: The biometric characteristic should lend itself to quantitative measurement in a practical manner.

Bolle, Connell, Pankanti, Ratha, and Senior (2004) argued that the biometric should also have a fifth attribute: acceptability, defined as “the particular user population and the public in general should have no strong objections to the measuring/collection of the biometric” (p. 6). Jain (2004) argued that a practical biometric system should consider the following two other attributes: (a) performance, which is “the achievable recognition accuracy and speed, the resources required to achieve the desired performance, as well as the operational and environmental factors that affect the performance”, and (b) circumvention, which “reflects how easily the system can be fooled using fraudulent methods” (Jain, 2004, p. 3).

#### *Identification versus verification*

One of the most important and fundamental distinctions of biometrics is found between the two authentication methods of verification and identification (Ashbourn, 2004; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chirillo & Blaul, 2003; Nanavati, Thieme, & Nanavati, 2002; Woodward, Orleans, & Higgins, 2003). Verification systems answer the question “Are you who you claim to be?” and involve confirming or denying an individual’s claimed identity. Identification systems, on the other hand, answer the question, “Who are you?” and involve establishing a person’s identity (Chirillo & Blaul, 2003).

In verification systems, the user claims an identity (e.g., a Windows username, a given name, an ID number) and provides biometric data (e.g., finger scan), which is compared against the user's enrolled biometric data. The answer returned by the system is that of "match" or "no match." Verification systems are referred to as 1:1 (one-to-one) systems because, while they may contain thousands or even millions of biometric records, they are "always predicated on a user's biometric data being matched against only his or her own enrolled biometric data" (Nanavati, Thieme, & Nanavati, 2002, p. 12). The process of providing a username and biometric data in biometric verification systems is called authentication. Bolle, Connell, Pankanti, Ratha, and Senior (2004) cautioned that verification systems do not provide "pure" biometric authentication because they rely on a combination of authentication modes – specifically biometric data compared against a unique identifier (e.g., ID number, user name).

Biometric identification systems, however, can be viewed as pure biometric authentication because identification is based only on biometric measurements (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). Whereas verification is referred to as a 1:1 system, identification systems are often referred to as 1:  $N$  (one-to- $N$  or one-to-many) because an individual's biometric information is compared against multiple ( $N$ ) records (Nanavati, Thieme, & Nanavati, 2002). Whereas verification systems return an answer of match or no match, identification systems return an identity (e.g., a name or ID number) as an answer. Identification systems are further divided into "positive" (designed to find a match for a user's biometric information in a database of biometric information, such as tracking individuals in a prison release program) and "negative" (designed to ensure that a

person's biometric information is *not* present in the database, such as preventing people from enrolling more than once in large-scale benefits programs). Although biometric identification systems are generally classified as 1: many applications, a scaled-back version of identification known as 1: few, a system that focuses on identification search against a small number of users is sometimes deployed.

Biometric identification systems are more difficult to design and implement than verification systems because of the extensive biometric database search capabilities needed (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). Additionally, identification systems are more subject to error than verification systems, because many more matches must be conducted, matches that increase the opportunity for error (Nanavati, Thieme, & Nanavati, 2002). Verification systems are overall much faster (often rendering a match/no match decision within less than a second) and more accurate than identification systems. Verification systems, as opposed to identification systems, predominate in private sector applications, particularly for computer and network security applications. Verification systems also predominate in applications designed to authenticate rights-to-access to buildings and rooms, although sometimes identification systems are also deployed in high-security environments. Identification systems are often found in public sector applications, such as law enforcement (i.e., parole and prison administration, forensics, etc.), large-scale public benefits programs (Nanavati, Thieme, & Nanavati, 2002), intelligence, and national security applications.

### *Application Areas*

While there are many potential applications for biometrics, the primary ones can be divided into the following three categories (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Nanavati, Thieme, & Nanavati, 2002):

*Physical access systems.* These systems “monitor, restrict, or grant movement of a person or object into or out of a specific area” (Nanavati, Thieme, & Nanavati, 2002, p. 14). In these systems, biometrics replace or complement keys, access cards, or security cards, allowing authorized users access to rooms, vaults, and other secure areas. Physical access systems are often deployed in major public infrastructure settings, such as airports, in order to monitor and restrict movements of unauthorized or suspicious persons. In addition to entry to secure rooms, physical access systems, when applied in business settings, include time-and-attendance systems by combining access to a location with an audit of when the authentication occurred.

*Logical access systems.* These systems “monitor, restrict, or grant access to data or information” (Nanavati, Thieme, & Nanavati, 2002, p. 14). Examples include accessing a computer or network or accessing an account. In logical access systems, biometrics replace or complement PINs, passwords, and tokens. Nanavati, Thieme, and Nanavati (2002) noted the following:

Because of the tremendous value of information stored on corporate networks and the transaction value of business-to-business (B2B) and business to consumer (B2C) e-commerce, the biometric industry views logical access as a much more lucrative industry segment in the long run than physical access. (p. 15)



*Ensuring uniqueness of individuals.* These biometric identification systems typically focus on preventing double enrollment in some programs or applications, such as a social benefits program (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). The main use of this application occurs in the public sector although similar systems could be implemented to prevent double enrollment in employee benefits programs.

#### *Central Components and Processes of Biometric Systems*

As Jain (2004) explained, “a biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database” (p. 3). The starting point for the biometric system is *enrollment*: a user’s biometric data is initially collected and processed into a template, the form in which it is then stored for ongoing use (Liu & Silverman, 2001; Prabhakar, Pankati, & Jain, 2003). As Woodward, Orlans, and Higgins (2003) explained that “templates are not raw data or the scanned images of a biometric sample, but rather they are an accumulation of the distinctive features extracted by the biometric system” (p. 37). Liu and Silverman (2001) described the template as “a mathematical representation of biometric data. A template can vary in size from 9 bytes for hand geometry to several thousand bytes for facial recognition” (p. 20). The templates are proprietary to each vendor and technology with little or no interoperability between systems. As Nanavati, Thieme, and Nanavati (2002) noted, this lack of interoperability is attractive from a privacy perspective but unattractive from the perspective of cost-effectiveness and the prospective implementer who is concerned about committing significant investment to a single non-standardized technology.

The term *presentation* refers to the process by which a user provides biometric data to an acquisition device by looking in the direction of a camera, placing a finger on a pad or sensor, or some other specified physiological exam. For purposes of verification or identification, the user presents biometric data, which is then processed and converted to a template. The scanned template is then matched against the stored enrollment template(s). Each time a user makes a presentation, a new template is created and matched. It is important to note, especially from the perspective of privacy concerns, that biometric systems do not store raw biometric data; instead they use the data for template creation and, in most cases, discard the biometric data. Moreover, as Nanavati, Thieme, and Nanavati (2002) noted:

Biometric data such as fingerprints and facial images cannot be reconstructed from biometric templates. Templates are not merely compressions of biometric data, but extractions of distinctive features. These features alone are not adequate to reconstruct the full biometric image or data. (p. 19)

The biometric system's match/no-match decisions are based on a score, which is "a number indicating the degree of similarity or correlation resulting from the comparison of enrollment and verification templates" (Nanavati, Thieme, & Nanavati, 2002, p. 20). Like the templates, the scoring system is based on proprietary algorithms; there is no standard system.

### Types of Biometric Technologies

As previously noted, biometrics can generally be grouped into two categories: physiological and behavioral. The International Biometric Group (IBG) provides data on comparative market share of various biometric technologies. The IBG data does not include

AFIS that is employed by law enforcement agencies. Instead it focuses on market share from other commercial and government applications. In 2004, the top four biometric technologies were all from the physiological category (see Table 1).

Table 1  
*Comparative Market Share of Biometric Technologies*

Biometric Technology	Market Share	
	2004	2003
Finger scan	48.0%	52.0%
Facial scan	12.0%	11.4%
Hand scan	11.0%	10.0%
Iris scan	9.0%	7.3%

*Note:* Sources are International Biometric Group (2005) for 2004 market share data and McHale (2003) for 2003 market share data.

The fifth most widely deployed biometric technology came from the behavioral category – voice scan, with a 6.0% share in 2004, an increase from 4.1% in 2003 (International Biometric Group, 2005; McHale, 2003). Each of these five biometrics is discussed in detail in the following sections.

#### *Finger Scan*

Finger scan or fingerprint technology is by far the most widely deployed biometric technology in the United States (Boroshok, 2005a; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chapple, 2003; Chirillo & Blaul, 2003; Lewis, 2005; Nanavati, Thieme, & Nanavati, 2002; Scheier, 2002). Finger scan's number one status as a biometric is maintained even if the extensive use of fingerprinting by law enforcement agencies is excluded. The type

of fingerprinting employed in commercial biometric systems differs from the one used in law enforcement. In most commercially available biometric applications, the station provides only for the scan of a single finger on one hand, whereas law enforcement agencies often rely on full sets of fingerprints. In addition to being the most widely used biometric, fingerprinting is also one of the oldest and most well researched biometric technology. Because it is a widely used, well-documented, and mature technology, costs for the deployment of finger-scan-based technologies are relatively low. Single-quantity pricing for a workstation version with associated software can be as low as \$150, while server versions are currently priced as low as \$50 per unit (Boroshok, 2005a; Lewis, 2005; Scheier, 2002).

*Strengths of finger scan.* The strengths of finger scan are one of the principal reasons for its popularity and include the following:

1. Widely used
2. Mature technology
3. Low cost
4. High ease of use (very little training is required to place a finger on a finger-pad)
5. Ergonomic design (comfortable to use for most users)
6. Low error incidence (false match rates are extremely low; crossover error rate is lower than voice scan and facial recognition, higher than hand geometry and iris scan)
7. Fast transaction times (in most systems, authentication takes less than a second)
8. Capacity to be deployed in a wide range of environments (e.g., on workstations, doorways, indoors/outdoors)
9. Ability to increase accuracy levels by enrolling multiple fingers

10. Can provide identification with a high level of accuracy (if properly configured to include multiple enrolled fingers) in addition to verification.

*Weaknesses of finger scan.* Despite its multiple strengths, finger scan is not without significant weaknesses. As Chirillo and Blaul (2003) noted, some of this technology's weaknesses stem from the same factors that lend it its strengths. "Because fingerprint technology is one of the oldest and most well-known technologies, a good amount of information is publicly available on how to defeat it" (p. 21). A number of ways exist to foil finger scans and produce a false match (false accept), including the use of a dummy finger constructed of latex or other material, manipulation of the scanner so as to raise the latent print of the person who used the scanner previously, and even use of an actual finger that is no longer attached to a body (most finger scanners cannot discriminate between live and dead tissue) (Chirillo & Blaul, 2003; Faundez-Zanuy, 2004). Because of these factors, the security levels of finger scans are not actually as impressive as the low error rates seem to indicate. It should be noted that countermeasures could be taken to overcome finger scan's vulnerability to fraud. For example, enrolling additional fingers makes fraud more difficult. To reduce the chance that the system will be foiled by synthetic or dismembered fingers, thermal scanners and/or moisture scanners can be added to the sensors to detect finger temperature and moisture levels that would indicate the vitality of the finger (Faundez-Zanuy, 2004). Other weaknesses include the following:

1. A scanner requires frequent maintenance because screens/sensors tend to retain an obstructing build-up of user skin oil and residue
2. Performance can deteriorate over time, both because of aging of the users (and

wearing away of fingertips) and because of the need for system maintenance

3. Finger scan biometrics are obviously not appropriate for users with missing hands or hand disabilities

4. Performance levels deteriorate among users who have hand tremors because the presentation of biometric data will be distorted

5. Performance levels also deteriorate when users' fingers are either overly dry (a certain amount of normal skin moisture is needed for an accurate reading) or overly moist/oily (as from too much hand lotion) (Feder, 2003)

6. There is a small but significant failure to enroll (FTE) rate even among a population with hands and without disabilities. The FTE rate for finger scans is estimated at 2–10% and is attributed to persons with genetically indistinct prints, scarred fingers, dry skin, and fingerprints worn down by age and/or manual labor (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Hill, 2001; Nanavati, Thieme, & Nanavati, 2002; "Prepare to be Scanned," 2003)

7. Perhaps the biggest weakness of finger scan, however, has nothing to do with the accuracy and reliability of the technology. Instead, it relates to user acceptance.

Because of finger scan's association with law enforcement and criminality, finger scans are often not readily accepted by users who dislike the technology's "taint" with forensic applications and who may worry that finger scan biometric data will be used for other purposes (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Hill, 2001; Nanavati, Thieme, & Nanavati, 2002; O'Gorman, 2003; Saccomano, 2003; Zhang, 2002)

8. According to Chirillo and Blaul (2003), “Another reason fingerprint technology is not highly accepted is that it may require individuals to share or touch the same device that others touch” (p. 24).

### *Facial Scan/Recognition*

Bolle, Connell, Pankanti, Ratha, and Senior (2004) noted that “face appearance is a particularly compelling biometric because it is one used every day by nearly everyone as the primary means for recognizing other humans. Because of its naturalness, face recognition is more acceptable than other biometrics” (p. 36). However, user acceptance of facial scans drops significantly when users discover that it has been used covertly (Imparato, 2002; Kaine, 2003; Nanavati, Thieme, & Nanavati, 2002). As Imparato (2002) recently observed, “Of all the biometric technologies currently in use, face recognition is arguably the most controversial” (p. 20). Kaine (2003) explained the working of face recognition biometric systems and their various applications as the following:

Facial Recognition (FR) is based on the computer identification of unknown face images by comparison with a database of known images. A Facial Recognition System (FRS) may be used for access control (one-to-one) or for surveillance of crowds to locate people of interest (one-to-many). Access control FRS are often used in highly controlled overt environments, which means that the input data is of predictable quality, resulting in relatively high levels of performance. However, surveillance applications are often covert and may call for a large number of faces to be compared with a large stored database of images to determine if there are any matches. (p. 315)

A variety of facial recognition technologies ranging from single image, video sequence, 3-D image, near infrared, to facial thermograms are available (Bolle, Connell, Pankanti, Ratha, & Senior, 2004).

*Strengths of facial recognition* include the following:

1. Capacity to leverage existing image acquisition equipment, such as digital cameras, Web, video, and the like
2. Because facial recognition is a software-based technology, it is often unnecessary to purchase new hardware, especially given the number of Closed Circuit Television (CCTV) and surveillance cameras in broad use (Nanavati, Thieme, & Nanavati, 2002)
3. The lack of need for specialized hardware can help keep the cost of this technology down, assuming that high software costs do not counterbalance the savings from the hardware (Soto, 2003)
4. It is the only biometric capable of identification at a distance without the subject's cooperation or even awareness (Nanavati, Thieme, & Nanavati, 2002)
5. Easy to use. All that is required is that the user (or target) look at the camera
6. Does *not* require the user to touch any device (a major objection for some users with finger scans and hand scans) (Chirillo & Blaul, 2003)
7. When deployed in verification situations, facial scans have extremely low failure-to-enroll rates (unlike fingerprints, human faces are almost always distinctive)
8. Capable of enrolling static images (e.g., photographs on driver's licenses), a factor which makes it possible to implement very large-scale enrollments at a relatively low cost and in a brief amount of time.



*Weaknesses of facial recognition.* Facial recognition systems have a number of serious weaknesses too. The predominant weakness (which derives from a combination of the technology's other weaknesses) is the appallingly low accuracy and high error rate of this biometric. Whether deployed covertly or overtly, facial recognition has the lowest accuracy rate among all five top biometrics (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chirillo & Blaul, 2003; Gips, 2002; Imparato, 2002; Kaine, 2003; Nanavati, Thieme, & Nanavati, 2002).

Evidence of the technology's low accuracy rate comes from a recent study at Palm Beach (Florida) International Airport that showed that the system failed more than 50% of the time to match the 15 employees who had enrolled in the database for a trial run. Out of 958 pass-throughs, the system matched the employees' faces just 455 times (Gips, 2002). Some studies suggest that accuracy improvements can be made in facial recognition systems, but these improvements will come at a very high cost. For example, Soto (2003) reported on a new facial recognition software package from Visionics FaceIt that resulted in impressively low error rates, as long as lighting conditions were perfect. The software cost \$30,000 for a three-camera system (Soto, 2003). Other weaknesses include the following:

1. False matches (false accepts) routinely occur in the case of twins, and most systems are insensitive enough for someone skillful at disguise and impersonation to "trick" the system into a false match
2. More likely than false matches, however, are false non-matches (false rejects) which can occur as a result of facial expressions, changes in hairstyle, changes in makeup, changes in facial hair, significant changes in body weight, eyeglasses, and

age-related facial changes (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chirillo & Blaul, 2003; Kaine, 2003; Nanavati, Thieme, & Nanavati, 2002)

3. The acquisition environment can have a dramatic impact on facial recognition system accuracy. In particular, lighting – either too bright or too dim – can dramatically increase the error rate

4. Perceived threat to privacy. Overtly deployed facial recognition technologies (e.g., used for identification and access) are generally judged relatively unobtrusive and meet with a high level of user acceptance. However, covertly deployed systems – such as those used for surveillance – pose significant threats to privacy. This is generally viewed as much more serious than that posed by the other top biometrics (Gips, 2002; Imparato, 2002; “Prepare to be Scanned,” 2003).

#### *Hand Geometry Scan*

Hand geometry scans refer not to handprints or to any analogy of fingerprints but rather to the geometric structure (or geometric invariants) of the human hand (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). Nanavati, Thieme, and Nanavati (2002) explained that “hand-scan technology utilizes the distinctive aspects of the hand – in particular, the height and width of the back of the hand and fingers – to verify the identity of individuals” (p. 99). The leading hardware maker for this technology, Recognition Systems, Inc. (RSI) has a basic hand scanner that takes upwards of 90 measurements from three to four enrollments to create a user template that includes length, width, and thickness, plus surface area of the hand and fingers. Newer systems include temperature-sensing mechanisms to ensure “live” subjects (Chirillo & Blaul, 2003). All the components of a hand scan system (acquisition hardware,

matching software, storage components) reside within a stand-alone device. Hand scans are a well-established biometric technology (they have been in widespread use since the 1970s), but compared to other leading biometrics, hand scans tend to be much more limited in their range of applications. Hand scans are used exclusively for verification rather than for identification because the hand measurements are not distinctive or specific enough to allow for identification applications and mostly for physical access and time-and-attendance applications (Nanavati, Thieme, & Nanavati, 2002). In the latter case they are used as a way to eliminate the problem of “buddy-punching” whereby one employee punches in or out for a coworker who is not present (Chirillo & Blaul, 2003).

*Strengths of hand scan.* Hand scan technology has changed very little since it was first introduced over 30 years ago, so its strengths and weaknesses are well established. The principal strengths of the hand scan include the following:

1. Operates in very challenging environments (the equipment is typically unaffected by light, dust, moisture, or temperature)
2. Established and reliable technology
3. Ease of use (users simply stick their hand in the unit, placement matters little)
4. Resistance to fraud compared to other biometrics (it would be difficult and time consuming to substitute a fake sample)
5. Small template size (as low as nine bytes – much smaller than other biometrics, allowing for storage of thousands of templates in a single unit)
6. Based on a relatively stable physiological characteristic
7. High level of user acceptance and lack of attached stigma (Bing, Zheng-ding, &

Dong-mei, 2002; Nanavati, Thieme, & Nanavati, 2002; Chirillo & Blaul, 2003).

*Weaknesses of the hand scan* include the following:

1. Limited accuracy (which in turn limits its use to verification not identification).

The relatively low accuracy of hand scan (higher than facial recognition and behavioral biometrics but lower than finger and iris scans) is a result of the general lack of physical variety expressed in the hand as well as the relatively small number of features measured by hand scan

2. Comparatively large form factor (this limits the technology's deployment in computer-oriented applications that require hardware with a smaller footprint)

3. Its ergonomic design limits its use by some populations (e.g., the disabled);

4. Comparatively high cost. At \$1,500 to \$2,000 per unit, hand scanners cost significantly more than finger scanners. Nanavati, Thieme, and Nanavati (2002) noted that the higher price of hand scanners "may be attributable to the lack of competition in the hand scan market" (p. 99).

### *Iris Scan*

Iris scan technology uses the unique pattern formed by the iris – the colored part of the eye bounded by the pupil and the sclera – to identify or verify the identity of individuals (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). The iris pattern is remarkably unique, for even in the same individual, no two irises are alike (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). The uniqueness of iris patterns has been likened to that of multilayered snowflakes. Chirillo and Blaul (2003) write that:

As is the case with retina and fingerprint technology, each iris pattern is unique. But unlike fingerprints, iris patterns contain much more unique data. This is partially because the iris is colored, but most simply due to the tremendous amount of unique patterns created by each iris. (p. 97)

The unique aspects of the iris make it an ideal biometric for high-security applications; enrolling both irises from the same individual can enhance the level of security. In addition to high-security physical access applications, iris scan technology has been used in ATMs and banking kiosks (Nanavati, Thieme, & Nanavati, 2002).

*Strengths of iris scan.* The most important strength of iris biometrics is its accuracy, the most critical weakness of facial scanning. Of all the leading biometrics, iris technology has the lowest error rate and the highest level of overall accuracy (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chirillo & Blaul, 2003; Nanavati, Thieme, & Nanavati, 2002; Soto, 2003). Other strengths of this biometric include the following:

1. Ability to be used both for verification and for identification
2. Stability of its biometric characteristics over a lifetime
3. Relatively difficult to fake or spoof because it is an internal biometric
4. The iris is minimally subject to outside influences when compared to biometrics like fingerprints and faces (Chirillo & Blaul, 2003; Nanavati, Thieme, & Nanavati, 2002; Sanchez-Reillo, Sanchez-Avila, & Gonzales-Marcos, 2000).

*Weaknesses of iris scan.* The major weaknesses of the iris biometric concern user perceptions and problems in the user-technology interface. Other weaknesses include the following:

1. Acquisition of the image requires moderate training and attentiveness: users must stand still and look straight into the scanner with eyes open and unblinking
2. Users often report some physical discomfort with the use of eye-based technology, although less so than with retina scanning technology
3. Anecdotal reports also suggest a fairly high level of user psychological resistance to iris-scanning technology, with some users believing that the scanner will lead to eye damage
4. Can be adversely affected by lighting and other environmental conditions (although not to the extent of facial scanning)
5. In some cases eyewear will adversely affect performance (although many iris devices can handle scanning people wearing glasses or contact lenses)
6. Although the iris is a relatively stable biometric, it is affected by aging and disease
7. Relies on proprietary hardware and software technologies
8. Costs tend to be high compared to finger scanning, hand scanning, and many facial recognition systems.

On the other hand, Soto (2003) reported that the per unit cost of the leading hardware/software combination technology has dropped to as low as \$300 per seat – still higher than finger scans but significantly lower than the over \$5,000 per seat price seen a few years ago.

### *Voice Recognition*

Voice recognition biometrics “utilizes the distinctive aspects of the voice to verify the identity of individuals” (Nanavati, Thieme, & Nanavati, 2002, p. 87). Voice recognition is

generally classified as a behavioral biometric, although it actually combines elements of behavioral and physiological biometrics: “The shape of the vocal tract determines to a large degree how a voice sounds, a user’s behavior determines what is spoken and in what fashion” (Nanavati, Thieme, & Nanavati, 2002, p. 87). Stated somewhat differently, “voice is a behavioral biometric but is dependent on underlying physical traits, which govern the type of speech signals we are able and likely to utter” (Bolle, Connell, Pankanti, Ratha, & Senior, 2004, p. 40). Because of comparatively low levels of accuracy and considerable user variability in voice dynamics, this biometric is generally used only for verification, not identification. Commonly deployed voice recognition systems can be divided into the following two types: (a) Text-dependent (the speaker is prompted to say a specific thing) systems and (b) Text-independent (the authentication system processes any utterances of the speaker) systems, which provide a higher level of security because they are more difficult to spoof and provide better accuracy than text-dependent systems.

*Strengths of voice recognition* include the following:

1. Capacity to leverage existing telephony infrastructure (as well as built-in computer microphones)
2. Low cost when existing infrastructure is used
3. Ease of use
4. Interface with speech recognition and verbal passwords
5. High level of user acceptance (this biometric is absent of negative perceptions associated with all of the other leading biometrics) (Nanavati, Thieme, & Nanavati, 2002; Teoh, Samad, & Hussain, 2003).

*Weaknesses of voice recognition* include the following:

1. More susceptible to replay attacks than other biometrics
2. Accuracy levels are low compared to iris scanning, finger scans, and hand scans
3. Accuracy levels are negatively affected by ambient noise and low-quality capture devices
4. Accuracy, security, and reliability are challenged by individual variations in voice, such as speaking softly or loudly, hoarseness or nasality because of a cold, etc.
5. The stability of the biometric is affected by illness, aging, and other user behaviors including smoking (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Nanavati, Thieme, & Nanavati, 2002; Teoh, Samad, & Hussain, 2003).

#### *Other Biometric Technologies*

The five major biometric technologies discussed above collectively comprise the vast majority of biometric technology under deployment. The only other biometric technologies that even register on market share breakdowns are two of the behavioral type: signature scan (2.4% share in 2003) and keystroke scan (0.3% share in 2003) (McHale, 2003). Although both of these behavioral biometrics are well accepted (signature scanning more so than keystroke scanning), their usefulness is limited by their lack of accuracy. Other behavioral biometrics under investigation include gait and lip motion (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Nixon, Carter, Grant, Gordon, & Hayfron-Acquah, 2003). One physiological biometric that has received considerable attention because of its high accuracy and security rates is retinal scanning. However, most analysts believe that the problems associated with retinal scanning (lack of user acceptance, high cost, difficult and painful acquisition process)



outweigh any advantages to this biometric. The general consensus seems to be that iris scanning has replaced retinal scanning as the eye scanning biometric of choice (Ashbourn, 2004; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; McHale, 2003; Nanavati, Thieme, & Nanavati, 2002; Hill, 2001; “Prepare to be Scanned,” 2003). The use of DNA as a biometric identifier has also been investigated, although it has significant weaknesses including the fact that it is portable and relatively intrusive to collect (Chirillo & Blaul, 2003). Other physiological biometrics that may prove useful in the future include body odor, skin reflectance (Bolle, Connell, Pankanti, Ratha, & Senior, 2004), and ear shape (Groves & Aston, 2004).

#### *Types of Errors and System Metrics*

Biometric verification systems make the following two types of errors (Ashbourn, 2004; Jain, 2004):

*False Accept.* Also known as False Match or Type 1 error: False Accept is the likelihood, expressed as a percentage, that an imposter will be matched to a valid user’s biometric (Liu & Silverman, 2001). In some systems – such as those that attempt to secure entry to a weapons facility, a bank vault, or a high-level system administrator account – the false match/false accept rate is the most important metric to watch. In other systems, such as a facial recognition system deployed by a casino in an effort to spot card counters, a high level of false matches may be tolerated.

*False Reject.* Also known as False Non-Match or Type 2 error: False Reject is the probability that “a user’s template will be incorrectly judged to *not* match his or her enrollment template” (Nanavati, Thieme, & Nanavati, 2002, p. 27). False non-matches

typically result in the user being locked out of the system. These false non-matches can occur because of changes in a user's biometric data, changes in how the biometric data is presented, and/or changes in the environment. Biometric systems are generally more susceptible to false rejects than they are to false accepts.

An important metric in biometric systems is the *Crossover Error Rate (CER)* -- also known as the Equal Error Rate (EER). This useful metric is the intersection of the False Accept and False Reject rates. In general, a lower CER indicates the biometric device is more accurate and reliable than another biometric device with a higher CER (Prabhakar, Pankanti, & Jain, 2003; Woodward, Orlans, & Higgins, 2003). Table 2 provides a summary of benchmark test-based accuracy/error rates for the five most prevalent biometric technologies. Each biometric technology is rank-ordered from most accurate to least accurate based on CER.

Table 2  
*Accuracy/Error Rates of Leading Biometric Technologies*

Biometric	False Match Rate	False No-Match Rate
Iris Scan	0.0001%	2.0%
Finger Scan	0.02%	2.0%
Hand Scan	0.3%	3.0%
Voice (text-independent)	7.0%	7.0%
Voice (text-dependent)	2.0%	0.03%
Face Scan	16.0%	16.0%

*Note:* Based on data contained in O'Gorman, 2003, p. 2032.

Another critical metric in biometric systems is the *Failure to Enroll (FTE)*. As Ashbourn (2004) explained, FTE refers to “a situation whereupon an individual is unable to enroll their biometric in order to create a template of suitable quality for subsequent automated operation” (p. 10). Common reasons for failure to enroll include physical disability and a user whose physiological/behavioral characteristics are less distinctive than average (Ashbourn, 2004). Nanavati, Thieme, and Nanavati (2002) observed that failure to enroll can be a major problem in “internal, employee-facing deployments” in which “high FTE rates are directly linked to increased security risks and increased system costs” (p. 35). A final important metric is the “transaction time”. Transaction time refers to “a theoretical time taken to match the live template against a reference sample” (Ashbourn, 2004, p. 10).

### Disadvantages and Problems with Biometric Technologies

#### *General Considerations*

Despite their many advantages over other commonly used authentication systems (as previously noted), the implementation of biometric authentication controls carries a number of risks and disadvantages. Even the most accurate biometric system is not perfect and errors will occur. The error rates and the types of errors will vary with specific biometrics deployed and the circumstances of deployment. Certain types of errors, such as false matches, may pose fundamental, critical risks to business security. Other types of errors – failure to enroll, false non-match – may reduce business productivity and efficiency and increase costs. Businesses planning biometrics implementation will need to consider the acceptable error threshold (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Harris & Yen, 2002; Kleist,

Riley, & Pearson, 2005; Woodward, Orlans, & Higgins, 2003). In any event, companies deploying biometric authentication systems must not be lulled into a belief that they are invulnerable to errors and/or fraud. Certain biometric systems (e.g., iris scanning) are fairly impervious to fraud, while others (especially behavior-based systems) are much more susceptible to it (Dunn, 2004; Jackson, 2002; “Prepare to be Scanned,” 2003). Facial scanning systems can be foiled with clothing, make-up, eyeglasses, and/or changes in hairstyle. Even relatively stable physiology-based biometrics like fingerprint scans can be defrauded with the use of rubber fingers and even through blowing warm air over the scanner and raising the latent print of the intruder’s predecessor (Dunn, 2004; Glass, 2004; Hogan, 2005).

The deployment of commonly used authentication systems (i.e., ID badges, passwords, etc.) requires relatively little training, although one could argue that better training on the development and use of passwords would improve security. This limited need for training is not the case with most of the most commonly used biometric systems. Both systems administrators and users need instruction and training to ensure smooth operation of the system. Some biometric systems are exquisitely sensitive to intra- and inter-user variation in presentation and performance. Their effectiveness becomes substantially compromised and error rates substantially increase in cases of significant variation and/or irregular presentation (Ashbourn, 2004; Chirillo & Blaul, 2003). A related problem concerns user acceptance of the biometric system. Some users may object to the deployment of biometrics out of concerns over privacy and intrusiveness (see the discussion below). In other instances, users may object to the deployment of biometrics and avoid optimal interface with the system because

of safety concerns, health concerns, general fears, and/or cultural and religious beliefs. For example, some individuals may be concerned that biometric systems that require them to touch a finger-pad or hand-pad will unnecessarily expose them to germs and place them at risk for illness. Some users may fear that eye scans will damage their eyes. Other users may object to eye scans on the basis that the eyes are the window to the soul (Chirillo & Blaul, 2003; Nanavati, Thieme, & Nanavati, 2002). Anderson (2001) noted that many Christian fundamentalists “are uneasy about biometric technology” because of its association with the mark of the Antichrist in Revelations 13:16-18 (p. 275).

Notwithstanding users’ beliefs and perceptions about the biometric system, in many cases features or elements related to the users and/or the operating environment will influence the successful implementation and effectiveness of the biometric system. Individuals with arthritis and/or certain other disabilities and physical limitations may be unable to enroll in systems and/or, subsequently, to align themselves physically in an optimal position with respect to biometric sensors. For example, the user with severe hand arthritis may be unable to place his/her hand firmly as required on the hand geometry sensor, and the user with migraines and associated photophobia may find it physically too uncomfortable to look straight into the light sensor for the iris scan. Some disabled people may simply have to be excluded from biometric systems altogether (Anderson, 2001; Ashbourn, 2004). Some relatively minor disabilities such as a slight tremor may compromise a legitimate user’s ability to gain access through certain biometric systems. Variation in physical size can also influence system accuracy. An iris scanner positioned for a standard height range may fail to capture images of either very short or very tall individuals, or in some cases an individual’s

hands/fingers may be either too large or too small to be read accurately in a hand or finger scanner. Likewise, individuals with neck and back problems may find it difficult to use some biometric devices, depending on the kind of positioning required of the user. Systems that rely on behavioral biometrics such as voice or signature are particularly vulnerable to variations and irregularities in user characteristics. For example, users who speak too softly, too loudly, or too rapidly may cause system errors. Minor changes in users' health could affect some biometric readings. Excessive skin moisture or lack of skin moisture can impact finger scans.

Although one of the ideal properties of a biometric is its universality, in reality not everyone has the characteristic or has it to the same degree. For example, some people are born without distinct fingerprints (Ashbourn, 2004). In other cases, users may have lost the distinctiveness of their fingerprints because of years of manual labor, use of certain chemicals, scarring, or the aging process (Anderson, 2001). Anderson (2001) noted that "people with dark-colored eyes and large pupils give poorer iris codes" (p. 274). Certain eye diseases and metabolic conditions may also reduce or negate the efficacy of eye scan authentication. Age has a significant impact on the user-biometric-system interface. Definite physiological changes are associated with the aging process. As Ashbourn (2004) observed,

The primary effect that these changes have upon the operation of biometric verification systems is one of poor template matching, as the live biometric may vary increasingly from the reference sample. This may necessitate reenrollment, perhaps a number of times over a given period. (p. 31)

Biometric-related properties most affected by the aging process include fingerprints because they become less distinct as the skin dries and becomes brittle with aging and also because wounds take longer to heal, and voice because of changes in tonal qualities and volume, and facial shape and appearance. Overall, the acceptability of a biometric system will be lessened if there is the impression that implementation of the system discriminates against or has an otherwise adverse impact on the disabled, the ill, ethnic minorities, the elderly, and/or other protected and/or traditionally disadvantaged groups of users.

A broad range of factors in the operating environment can also impact the effectiveness and acceptability of biometric systems. User-related cultural, social, and behavioral factors can influence the system performance (Ashbourn, 2004; Chirillo & Blaul, 2003; Nanavati, Thieme, & Nanavati, 2002). For instance, the accuracy of facial scans can be compromised by users' changes in hairstyle, facial hair, and headwear as well as by changes in an individual's physical appearance because of significant weight gain or loss. The accuracy of voice/speech recognition systems is affected by the distance between the scanner and the user, as well as by the volume of speech. Fingerprint recognition is impeded in cases when users' skin is too dry, whether the condition arises as a result of aging, skin disease, environmental factors, or occupation-related factors, such as frequent hand washing among healthcare professionals (Ashbourn, 2004; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Ratha, Connell, & Bolle, 2001). Factors in the surrounding ambient environment may also affect the accuracy of the biometric system. Ambient lighting will influence accuracy and error rate in facial scans and, to a lesser extent, in iris scans. Noise levels can impede the effectiveness of voice recognition systems. Humidity and air temperature can affect the

accuracy of fingerprint and hand scans (Ashbourn, 2004).

Although the cost of biometric system implementation has fallen dramatically in the past few years, it is still a major barrier for many companies (Dunstone, 2001; Hulme, 2003; Hurley, 2003; Liu & Silverman, 2001; Vijayan, 2004;). Costs vary significantly depending on the type of system. Recent reports suggest that newer fingerprint scanners can be purchased for as little as \$50 per unit, while voice recognition systems can cost in excess of \$50,000 (Dunstone, 2001; Lewis, 2005; Matyas & Riha, 2003). However, even the least expensive biometrics systems are likely to cost more than simpler versions of traditional authentication systems with experts estimating minimum costs, including hardware and software, at \$200 or so per user and upwards of \$150,000 for corporate-wide protection in a medium-sized business (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Chirillo & Blaul, 2003; Harris & Yen, 2002; O’Gorman, 2003). Compounding the cost issues are problems related to the lack of clear standards and the lack of clear interoperability between various biometric authentication systems (Costlow, 2003; Jackson, 2002).

Many of the problems and difficulties with biometrics systems are likely to be corrected or significantly mitigated with technological improvements, better user and administrator training, and good control of environmental conditions. In other cases, problems can be overcome or ameliorated with the use of countermeasures such as combining different types of biometrics, combining biometrics with traditional authentication systems, etc. Two major concerns that will continue to loom large and deserve closer examination are biometric identity theft and user privacy.



*Biometric Identity Theft*

Although biometrics are much less vulnerable to theft than other authentication controls, they are not immune to this danger. Moreover, when a biometric identity is stolen, it creates a much bigger problem than that created by the theft of an ID badge, USB key, or password (Dunstone, 2001). When an imposter or intruder defrauds a biometric authentication system and creates a false match error, he/she not only defrauds the entire biometric security system, he/she compromises the individual authorized user's biometric integrity. As Ratha, Connell, and Bolle (2001) observed:

One of the properties that makes biometrics so attractive for authentication purposes – their invariance over time – is also one of its liabilities. When a credit card number is compromised, the issuing bank can just assign the customer a new credit card number. When the biometric data are compromised, replacement is not possible. (p. 620)

Likewise, Prabhakar, Pankanti, and Jain (2003) noted, “One disadvantage of biometrics is that they cannot be easily revoked. If a biometric is ever compromised, it is compromised forever” (p. 39). Hamilton (2003) made a similar observation:

If the system is breached, that raises some difficult problems. Lose a smart card or a photo ID, and it's relatively easy to cancel the old card and issue a new one, with the only cost being temporary inconvenience. Discover that a stranger has somehow managed to pass herself off as you by forging the electronic representation of your handprint, and your options are extremely limited. You are unlikely to grow a new hand. “Once someone steals your biometric, it remains stolen for life,” says Bruce

Schneier, a security expert who founded Counterpane Internet Security Inc. in Cupertino, California. (p. R4)

A number of analysts believe that the ultimate solution to the problem of biometric identity theft lies in the development of “cancelable biometrics” (“Biometrics, Trusted Computing Key,” 2004; Dunstone, 2001; Ratha, Connell, & Bolle, 2001). Researchers at IBM have developed a prototype for the cancelable biometric. They described it as follows:

It consists of an intentional, repeatable distortion of a biometric signal based on a chosen transform. The biometric signal is distorted in the same fashion at each presentation, for enrollment and for every authentication. With this approach, every instance of enrollment can use a different transform thus rendering cross-matching impossible. Furthermore, if one variant of the transformed biometric data is compromised, then the transform function can simply be changed to create a new variant (transformed representation) for re-enrollment as, essentially, a new person. (Ratha, Connell, & Bolle, 2001, p. 620)

### *Privacy Concerns*

The use of biometric authentication controls raises significant privacy concerns, particularly in comparison to conventional authentication methods like passwords and ID badges (Alterman, 2003; Bolle, Connell, Pankanti, Ratha, & Senior, 2004; McHale, 2003; Nanavati, Thieme, & Nanavati, 2002; Rupley, 2002; Woodward, Orleans, & Higgins, 2003). User objections to biometrics are often based on privacy concerns, sometimes articulated in terms of the user’s sense of the intrusiveness of the biometric system. Anecdotal reports suggest that public perceptions of intrusiveness vary among different biometrics and in how

biometrics are implemented. With regard to the latter, Nanavati, Thieme, and Nanavati (2002) reported that there is a greater risk of privacy invasiveness when:

1. Deployment is covert (users are not aware of the system's operation) versus overt
2. The system is mandatory versus opt-in
3. The system is used for identification rather than verification
4. It is deployed for an indefinite duration versus fixed duration
5. It is deployed in the public versus private sector
6. The user is interfacing with the system as an employee/citizen versus individual/customer
7. An institution versus the user owns the biometric information
8. The biometric data is stored in a template database versus the user's personal storage
9. The system stores identifiable biometric data versus templates.

A vivid example of the public's lack of acceptance of the covert use of biometric systems comes from the 2001 Super Bowl and the uproar that ensued after the Tampa Police Department deployed facial scanning technology for the purpose of picking out criminal suspects from the audience (Alterman, 2003). In contrast, in the aftermath of September 11, there is fairly widespread public acceptance of the use of facial scanning at airports.

Users generally view behavior-based biometrics such as voice recognition and signature verification as less intrusive and less privacy-threatening than physiology-based biometrics (Nanavati, Thieme, & Nanavati, 2002; Woodward, Orlans, & Higgins, 2003). Facial scanning is typically viewed as having a high potential for privacy invasion because of

the capacity to deploy it without the user's knowledge and participation. Finger scans may be viewed as intrusive and privacy-invasive because of their association with law enforcement functions. The level of intrusiveness of the scanning technique appears to affect users' perception of privacy invasion, with iris scanning provoking more privacy objections than hand scanning (Nanavati, Thieme, & Nanavati, 2002). Civil libertarians and users also raise privacy objections over biometric systems that have the potential to uncover additional information about the user beyond the biometric identity. For example, finger scans, because of their capacity to be linked to large law enforcement databases of fingerprints, could be used to reveal information about the user's criminal background. Iris scans have the capacity to reveal confidential medical/health information about the user (Nanavati, Thieme, & Nanavati, 2002; Woodward, Orleans, & Higgins, 2003). Probably one of the most troubling privacy-related aspects of biometrics is the potential for large-scale linkage between biometric systems and the use of biometric data to facilitate large scale national ID programs (Alterman, 2003; Nanavati, Thieme, & Nanavati, 2002; Rupley, 2002; Woodward, Orleans, & Higgins, 2003). Even though employers may design a biometric system for purely in-house use in order to facilitate verification of employee identities on corporate networks, federal regulations and laws such as the USA PATRIOT Act may eventually compel the employer to surrender employees' private biometric data to government authorities (Alterman, 2003; Rupley, 2002; Woodward, Orleans, & Higgins, 2003).

In summary, the major privacy concerns associated with biometric deployments include the users' loss of anonymity and autonomy, the risk of unauthorized use of biometric information and/or unauthorized collection of biometric information, the unnecessary

collection of biometric information, the unauthorized disclosure of biometric information to others, the systematic reduction of users' reasonable expectation of privacy, and the creation of a real-life "Big Brother" scenario (Nanavati, Thieme, & Nanavati, 2002; Woodward, Orlans, & Higgins, 2003). Many of these concerns can be generally lumped under the heading of "function creep." As Woodward, Orlans, and Higgins (2003) explained,

What would inevitably happen over time, according to civil libertarians, is a phenomenon known as "function creep" or "mission creep": identification systems incorporating biometrics would gradually spread to additional purposes not announced or not even intended when the identification systems were originally implemented. The classic example of function creep is the use of the Social Security Number (SSN) ... the original Social Security cards containing the SSN bore the legend, "Not for Identification"... By 1961, the IRS began using the SSN for tax identification purposes. By 2002, countless transactions from credit to employment to insurance to many states' drivers licenses require a Social Security Number and countless private organizations ask for it even when it is not needed specifically for the transaction at hand. (p. 208)

Notwithstanding the privacy risks, supporters of biometric authentication systems argue that properly deployed and with adequate best practice controls, biometric systems can actually function to enhance and protect privacy (Nanavati, Thieme, & Nanavati, 2002; Woodward, Orlans, & Higgins, 2003). Woodward, Orlans, & Higgins (2003) pointed out that "several newly developed biometric technologies use an individual's physical characteristics to construct a digital code for the individual without storing the actual physical

characteristics,” thus creating a sort of *biometric encryption* that can be used to protect the privacy of an individual’s financial, medical, or other data (p. 211). Nanavati, Thieme, and Nanavati (2002) argued that “privacy-sympathetic” biometric systems can be designed. Such systems would have the following characteristics:

1. Limited system scope
2. Eschew use of biometrics as a unique identifier
3. Limit retention of biometric information
4. Limit storage of identifiable biometric data
5. Limit collection and storage of extraneous information, include “opt-out” provisions for users
6. Enable anonymous enrollment and verification
7. Provide means of correcting and accessing biometric-related information
8. Limit system access
9. Use security tools and access policies to protect biometric information
10. Make provisions for third-party audits
11. Disclose the system purpose and objective
12. Disclose enrollment, verification, and identification processes
13. Disclose policies and protections in place to ensure privacy of biometric information
14. Disclose provisions for system termination (Nanavati, Thieme, & Nanavati, 2002).

In contrast to this view, Alterman (2003) argued that the deployment of biometric

systems and the use of biometric data for identification and verification are ethically questionable because they always entail a violation of privacy and autonomy. Alterman (2003) found “something disturbing about the generalized use of biometric identification apart from the standard data privacy issue” (p. 143). He explained that,

This view is based on the claim that privacy is control over how and when we are represented to others. The proliferation of representations that identify us uniquely thus involves a loss of privacy, and a threat to the self-respect which privacy rights preserve. I think we should be wary when an author writes that “increasingly, the way to keep information secure is to offer up a piece of yourself ... to be recorded and used to verify your identity”. My concern is that the metaphysical “piece of yourself” that is offered up may be important to retain control over and hard to recapture once it is put in the form of a proprietary digital image. (Alterman, 2003, p. 143)

Alterman (2003) maintained that biometric data “has inherent moral value” (p. 145). He did not go so far as to argue against *any* deployment of biometric identification or verification systems. Rather, he maintained that they must be judiciously implemented and only deployed with due consideration to users’ privacy concerns. Alterman wrote that

We have both general and special privacy interests in biometric images. This means that privacy is a tradeoff in the use of biometric identification, not that there are no valid uses of such systems ... My main conclusion is that the general right to privacy includes the right to control the creation and use of biometric images of ourselves. This right must be a “presumption”... therefore derogations of it must be grounded by compelling considerations of public safety or other important norms. It follows from

this that we should carefully consider the decision to make biometric images of our bodies available to others. (Alterman, 2003, p. 147)

## Biometrics in Action

### *Overview of Recent Trends in Biometric Authentication*

#### *Government advances in biometric authentication*

Although private sector organizations are increasingly adopting biometric technologies for their authentication needs, the government (public) sector has led investment in biometrics. September 11 and the USA PATRIOT Act have encouraged increasing government commitment to biometric technologies (“Government Catches Biometrics Bug,” 2005; McHale, 2003). The Department of Defense, the Department of Homeland Security, the Immigration and Naturalization Service, and the Department of Transportation are the government agencies most involved in the deployment of biometrics technologies. The Department of Defense’s (DOD’s) Common Access Card (CAC) program involves putting biometric technology on a smart ID card. The DOD also recently acquired 1,300 U.areU. Pro fingerprint recognition systems in order to enhance network security at workstations in its offices in the Washington D.C. metropolitan area (McHale, 2003). The US-VISIT program under the Department of Homeland Security is another government program that incorporates biometrics (including face and fingerprint) into a smart ID card (McHale, 2003). Another Department of Homeland Security program, the Transportation Worker Identity Credential (TWIC) incorporates biometric information in an ID card (“Government Catches Biometrics Bug,” 2005).



*Face scanning at airports*

After the September 11 terrorists' attacks, most of the nation's airports moved to incorporate face-scanning technologies into their security systems. Most studies of the effectiveness of these systems, however, have revealed their high error rates and low accuracy rates (Murphy & Bray, 2003; Schwartz & Huddart, 2004).

*Increased deployment in the financial industry*

Usually slow to embrace new technologies, the financial industry has actually been one of the leaders in the adoption of biometric authentication controls ("Banking on Biometrics," 2004; "Bringing Biometrics to e-Commerce," 2003; Kresbsbach, 2003; Ward, 2004). Current deployments range from fingerprint scanners securing computer networks for brokers to facial recognition systems at ATMs to iris scanning for high-security access points. International Biometric Group projects that U.S. financial services firms will spend \$672 million in 2007 for various biometric deployments (Kresbsbach, 2003). One of the biggest deployments to date has been United Bankers' Bancorporation (UBB) adoption of U.are U.Online, a fingerprint recognition system that allows UBB customers to automatically log onto UBB's Web site with finger scans versus passwords (Ward, 2004). UBB also adopted a fingerprint authentication system for its employees ("Biometrics are Opening Many Eyes," 2004). Wells Fargo, Bloomberg Financial, and Janus Capital Management are other well-known financial firms that have adopted biometric authentication systems for employees and/or customers. While some financial institutions have selected voice, iris, or facial-scan-based systems, most seem to be choosing finger scan systems.

*Biometrics in the healthcare industry*

Spurred in part by new regulations that require healthcare institutions to ensure the privacy and security of patient records, healthcare companies have also been at the forefront in the adoption of biometric authentication (“Beyond Doors: Securing Records with Finger Flick,” 2002; Hulme, 2003; Messmer, 2002; Morrissey, 2002; Reynolds, 2004). Among the major healthcare organizations that have moved to biometric authentication is the Mayo Clinic, which adopted a fingerprint ID system in 2002 (Morrissey, 2002). The majority of healthcare institutions that have adopted biometric authentication systems have selected finger scan ID systems. However, deployment of these systems in healthcare organizations has not met with the same success as seen in the financial services industry. Error rates have been higher and accuracy rates much lower than expected. The major reason behind the high incidence of errors appears to be the particulars of the healthcare environment, especially the characteristics of the hands of the doctors, nurses, and other healthcare workers using these systems. Specifically, system performance appears to be undermined by the chronically dry hands of these workers, a condition resulting from frequent hand washing and the use of alcohol-based hand sanitizers. Another problem has been the resistance to using the fingerprint technology by both nurses and doctors, who feel that it involves a privacy intrusion.

*Increased deployment of time and attendance systems*

A review of the literature suggested that an increasing number of companies across many different industries are deploying biometric-based time-and-attendance systems (Gurliacci, 2004; Hannah, 2005; Kilborn, 2002; Liddle, 2004; Maher, 2003; Morris, 2002;

“Plant Access with Biometrics,” 2003; Roberts, 2003). A shift from the past practice is in the increased use of biometric attendance and tracking systems for white-collar workers.

Previously the focus was on blue-collar factory workers. Although some employers are using the traditional hand-scanning systems, there appears to be a shift towards the use of finger-scanning time-and-attendance systems. This shift seems to be related to the more competitive pricing structure for the finger-scanning systems.

#### Advantages and Disadvantages of the Various Biometric Technologies

There is no universal “best” biometric authentication system. Each of the five leading biometric technologies carries specific advantages and disadvantages. Some biometric technologies are more appropriate for certain applications and environments than their counterparts. An organization in the midst of evaluating potential biometrics authentication implementation must recognize that there will be trade-offs in any selection, such as cost for accuracy, privacy versus user acceptance, etc., and there are not yet any universal decision factors for selecting a particular biometric technology for a specific application. There is, however, substantial research into many of the advantages and disadvantages of biometrics. Table 3 provides a summarized comparison of the features of the five leading biometric technologies analyzed in this dissertation. The features, shown in the extreme left column, were excerpted from various researcher efforts and the rankings represent an amalgam of the rankings found in the literature (Bolle, Connell, Pankanti, Ratha, & Senior, 2004; Harris & Yen, 2002; Kleist, Riley & Pearson, 2005; Woodward, Orlans, & Higgins, 2003).

Table 3a  
*Comparison of Leading Biometric Technologies*

	Finger Scan	Facial Scan	Hand Scan	Iris Scan	Voice Recognition
Accuracy	High	Low	Medium	Very High	Low to Medium
Ease of Use	High	Medium	High	Low to Medium	High
User Acceptance	Medium	High (overt) Low (covert)	High	Low to Medium	High
Privacy Concerns	High	Very High (overt)	Medium	High	Very Low
Cost	Low to Medium	Low to Medium	Medium	High	Low
Performance	High	Low	Medium	High	Low
Potential for Circumvention	Medium	High	Low to Medium	Very Low	High
Distinctiveness	High	Low	Medium	Very High	Low
Barriers to Universality	Worn ridges; hand or finer impairment	None	Hand impairment	Visual impairment	Speech impairment
Susceptibility to Changes in Biometric	Low to Medium	Medium to High	Medium	Low	Low to Medium
Susceptibility to Changes in the Environment	Low	High	Very Low	Low	Medium to High

Table 3b  
*Comparison of Leading Biometric Technologies*

	Finger Scan	Facial Scan	Hand Scan	Iris Scan	Voice Recognition
Error-causing Factors	Age, trauma, degradation of prints	Lighting, contrast, pose, movement, expression	Hand injury or trauma, inability to place correctly	Positioning, eye angle, glasses, disease	Illness, age, quality of communication system, ambient noise
Mitigations for Potential Errors	Periodic reenrollment, enrollment of multiple fingers	Frequent reenrollment, multiple scans, controlled environment	Periodic reenrollment, enrollment of both hands	Periodic reenrollment, user training, enroll both irises	Periodic reenrollment, control ambient noise

### Summary and Recommendations for Considering Biometrics

Recent literature has shown that while biometric authentication systems promise cost savings and higher levels of security for businesses, they are not a panacea. Many different factors affect how well or how poorly biometric authentication controls will perform in any given organizational environment. Included among these factors are the users, the administration, the environment, the infrastructure, the budget, the communication system, and the existing security needs (Harris & Yen, 2002; Kleist, Riley & Pearson, 2005). While many biometric technologies are capable of operating as stand-alone systems, in reality their accuracy and performance levels would be greatly improved by combining them with more conventional authentication methods such as passwords and keys (Callas, 2003; Gianus, 2003; Jonietz, 2004; Kolodgy, 2003; Margulius, 2004).

In selecting a biometric authentication system and preparing for its implementation, organizations should focus closely on the user-technology interface and the conditions in the organizational environment that may influence the technology's performance. For example, the healthcare industry's unreflective embrace of finger scan technology illustrates the dangers of failing to heed environmental realities. It is important that organizations consider not only the practical impediments to effective implementation but also the potential psychological impediments such as user fears about the technology. Ethically, the organization also has the obligation to consider carefully the extent to which the implementation of biometric authentication compromises the privacy rights of users. In making this assessment, management must take into account the possibility that the organization may be compelled to release employees' biometric-related information to

government authorities.

### Gaps in the Literature Regarding Biometrics

A review of the recent literature on the adoption of biometric technologies in organizations revealed almost no research regarding the factors influencing the decision to implement biometric access technologies. Research into this area could help explain why organizations are reluctant to implement biometric authentication controls. It could also help IT and security decision makers to determine what aspects of biometric security technologies are of concern to them and accordingly recommend appropriate security solutions for their organizations. Security technology companies can also benefit from this research by knowing what is important to their customer base while introducing new IT security products and/or technologies. Although there is a dearth of scholarly research regarding the factors influencing the decision to recommend or not recommend biometrics, there is a solid foundation of theories and previous studies on technology adoption in general. The next section of this literature review explores the decision making process and discusses the origins and development of the dependent variables used in this study.

### Section 2: Organizational Decision Making Overview

Although not directly studied as part of this research effort, a review of the literature would be remiss if it did not include a discussion of organizational decision making because ultimately the IT/IA manager's decision to recommend or not to recommend biometric security technologies impacts any organizational decision regarding the adoption of

biometrics. Unfortunately, the literature focusing on organizational decision making has not yet fully arrived at any definitive theory agreeable to the majority of researchers and theorists in the organizational studies space. Some researchers have emphasized that organizational decisions are based on the notions of rationality and optimality, while others argue that decision making processes in organizations are haphazard, uncertain, and full of ambiguity (Cohen, March, & Olsen, 1972; Harrison, 1998; Isenberg, 1984; Mintzberg, Raisinghani, & Theoret, 1976; Schlaifer, 1959; Simon, 1955). The extensive stream of research on organizational decision making indicates a diversity of research disciplines used in the study of decision making. It is commonly acknowledged that scholars and practitioners involved in decision making differ significantly in their concepts, approaches, methods, and applications.

Ungson and Braunstein (1999) contend that research in organizational decision making focuses on contextual associations underlying decision making in groups and organizations but lacks the experimental controls necessarily to examine rigorously these associations. There is little cross-referencing in the research literature among researchers of behavioral decision making, human problem-solving, and organizational decision making. This lack of integration is not surprising because the research fields differ in methodology, levels of analysis, and epistemology. The proliferation of labels in the field of decision making (e.g., behavioral decision making, decision theory, human information processing, judgment theory) is testimony of the growing divergence and complexity of decision making research (Abelson, 1976; Dawes, 1979; Hammond, McClelland, & Mumpower, 1980; Henderson & Nutt, 1978; March & Olsen, 1976; Mintzberg, Raisinghani, & Theoret, 1976;



Mitroff & Emshoff, 1979; Newell & Simon, 1972; Simon & Hayes, 1976; Tuggle & Gerwin, 1980; Tversky & Kahneman, 1974).

The literature on theories of decision making can be divided into the following two distinct fields: (a) behavioral decision theory and (b) organizational decision theory.

According to March and Shapira (1999), these two fields of decision making are different, yet they have a history of conspicuous cross-pollination. Some of the early work in organizational decision theory was, in a very general way, an effort to represent decision making in organizations as intentionally rational and subject to rather severe cognitive constraints (Simon, 1955; Tversky & Kahneman, 1974). These studies of decision making regarding new technologies are essentially examinations of the extent to which individuals treat preferences, expectations, and perceptions.

Some of the early work in behavioral decision theory was affected by speculation about organizations. In fact, researchers and observers of decision making move back and forth rather easily from discussions of individual decision making to discussions of organizational decision making and use many of the same concepts for both. Rational models see decisions as being made by the evaluation of alternatives in terms of their future consequences for prior preferences. A large portion of the literature discussing the theoretical developments in the analysis of decision response – both at the individual and the organizational levels – is some form of elaboration of that underlying vision of willful human action. In studies of both individuals and organizations, there is a persistent fascination with the extent to which decision making reflects processes and produces outcomes familiar to the modern decision scientists.

*Decision Processes and Influential Factors*

The decision to adopt a proposed new technology is not made instantaneously by individual decision makers in organizations. The decision to recommend a new technology initiates a series of processes within an organization. The adoption process of a recommended new technology infiltrates an organization, moves between social units, and passes through such phases as awareness, evaluation, adoption, utilization, and institutionalization (Beyer & Trice, 1978; Ettlie & Vallenga, 1979). According to most technology adoption models, an organization's attitudes toward new technology affect the process of adopting the technology (Lavidge & Steiner, 1961; Rogers, 2003).

Some researchers have indicated that the assimilation of innovative new technologies into organizations is a process unfolding in a series to evaluate, adopt, and implement these technologies (Meyer & Goes, 1988). Everett M. Rogers (2003) has defined five stages of the innovation adoption decision process as the following: (a) knowledge of an innovation, (b) perception of the innovation formed, (c) decision to recommend/adopt or not recommend/adopt the innovation, (d) implementation of the innovation, and (e) confirmation of the decision. The critical decision factors influencing the second and third stages were the focus of this study.

However the decision process is defined, researchers have identified a myriad of factors influencing the decision processes involved in recommending a new technology for adoption or implementation in an organization. Notably, organizational leaders charged with the responsibility of organizational IT adoption decisions typically take into account the extent to which the IT under consideration will "fit" with the capabilities and needs of the

organization (Dasgupta, Agarwal, Ioannidis, & Gopalakrishnan, 1999; Duxbury, Decady, & Tse, 2002; Grover, Teng & Fielder, 1998; Khazanchi, 2005; Lai & Guynes, 1997). Ettlie (2000) proposed that the factors that influence these processes be divided into three categories. First, the attributes of a new technology itself influence the decision processes. Examples of factors in this category involve function-effectiveness (the ability of the new technology to function “as-advertised”), reliability, and cost-effectiveness. The second broad category of factors consists of the characteristics of organizational requirements and perceived need for the new technology. The third category of factors comprises the context or environment of the organization. These factors may involve suppliers, customers, and economic resources of the firm. Similar to Ettlie’s (2000) findings, Koch (2002) argues that the soundest organizational decisions on IT adoption are those that consider IT investments in the context of the overall organizational strategy. He argues that IT investments must be linked with organizational strategy and specific core business processes. Vogel (2004) agrees, noting, “IT strategic planning isn’t just about technology” (p. 92).

Roberts and Pick (2004) found security and reliability to be the most important factors influencing technology adoption and cost-effectiveness to be a moderate factor. In its continuing research on organizational IT security risks and organizational decision making in IT security adoption, the Tuck Business School’s Center for Digital Strategies (2005) identified organizational need factors as the drivers of organizational IT security adoption. Bergstrom (1987) also emphasized that organizational needs influence the decision processes involving new technologies. Putnam (1987) points out that the success of a modernization project in organizations where new technologies are involved may be impacted by the

following critical factors: (a) organizational needs, (b) cost-effectiveness, (c) reliability, and (d) appropriate functioning of the new technology (function-effectiveness). Quantz (1984) proposed that the availability of a new technology “champion” is an important factor for the successful adoption of a new technology.

#### *Attitudes and Perceptions as Factors in Decision Making*

Researchers who have examined the problem of new IT adoption have drawn extensively from theories developed in innovation adoption and in social psychology with a number of models proposed to guide inquiry into this phenomenon (Agarwal & Prasad, 2000, 1998; Ajzen, 1988; Brancheau & Wetherbe, 1990; Davis, 1989; Kwon & Zmud, 1987; Rogers, 2003). Despite the existence of these models and the many divergences in hypothesized associations, a common theme underlying these models is the inclusion of perceptions of a new technology as independent variables. Everett M. Rogers’ (2003) model of the diffusion of innovations portrays attitudes toward a new technology as antecedents to the decision to adopt the new technology. Fred Davis’s (1989) technology acceptance model and its precursor, the theory of reasoned action (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975), both postulate that attitudes or perceptions about a technology are instrumental in the decision to adopt the technology.

Attitudes towards technologies are formed based on the perceptions of the attributes relevant to the specific use of a technology. Once attitudes are established, they are relatively stable because existing beliefs serve to mediate and filter new information (Young, 1972). Perceptions related to the attributes of a technology can either enhance or diminish the acceptability of the technology, depending on the values of those doing the perceiving. In

other words, individuals can characterize a technology by any set of attributes that they have come to associate with the technology.

Otway and Haastrup (1989) contend that technologies in organizations are judged and accepted or rejected on the basis of a complete package of perceptions about them. Research on the “perception” of technological attributes has taken two main approaches. One approach is to have respondents rate a large number of different technologies on the same set of attributes to see how perceptions differed in the resulting factor space (Fischhoff, 1978). The other approach (Otway, Maurer, & Thomas, 1978) is to study attitudes toward specific technologies in depth (or alternate technologies intended to provide the same benefits) as a function of the underlying beliefs and values of the respondents. Otway and Haastrup (1989) indicated that the results of the two methods are in broad, general agreement.

Otway and Haastrup (1989) also indicated that the general attitude towards a new technology in an organization depends on the level of effective communications between technical staff and end users. These researchers contend that an organization’s overall attitude toward the adoption of a new technology depends on its employees’ perceptions of the new technology. In this sense, the perceptions of the attributes of a specific technology and the attitudes of both technical staff and end users in an organization become a legitimate part of the decision making process.

### Gaps in the Literature Regarding Decision Making

As previously discussed, the review of the recent literature on the adoption of biometric technologies revealed almost no research regarding the factors influencing the

decision to implement biometric access technologies. The literature review suggests that there is also a major gap in the research relating to organizational decision processes focusing on recommending or not recommending new technologies in organizations. Many researchers have pointed out the need for a better understanding of the decision making process for adopting new technologies in organizations (Collins, Mage, & Hull, 1988; Downs & Mohar, 1976; Dynes, Brechbuhl, & Johnson, 2005; Ettl, 2000, 1986, 1979; Kelly & Kranzberg, 1978; Kimberly & Evanisko, 1981; Meyer & Goes, 1988; Roberts & Pick, 2004). However, few studies have examined the decision processes that precede recommendation or adoption (Kimberly, 1981; Tornatzky, Eveland, Boylan, Hetzner, Johnson, Reitman, & Schneider, 1983).

Comparative studies to date have not arrived at consistent conclusions. These studies examined various categories of predictor variables in the context of specific new technologies as well as organizations in specific industries. A few case studies have attempted to address this research issue. However, the focus of these studies was on a specific new technology within the context of an organization that had successfully implemented the technology and not on the decision factors that influenced the decision to recommend or adopt the technology (Beyer & Trice, 1978; Craig & Hamidi-Noori, 1985; Collins, Hage, & Hull, 1988; Daft & Becker, 1981; Meyer & Goes, 1988; Hamidi-Noori & Templer, 1983).

#### *Research recommendation*

As discussed previously, organizational decision making can be quite complicated when considering the adoption of new security technologies. Biometrics have capabilities,

features, and challenges that can make the decision to recommend or not to recommend the technology even more difficult. Consequently, research into the factors that influence a manager's decision to recommend or not to recommend biometric security technologies could help explain why companies have been reluctant to implement biometric authentication controls. It could also help IT and security decision makers to determine what aspects of biometric security technologies are of concern to them and recommend accordingly appropriate security solutions for their organizations. Security technology companies can also benefit from this research by knowing what is important to their customer base while introducing new IT security products and/or technologies.

## CHAPTER 3. METHODOLOGY

### Theoretical Framework

The purpose of this study is to help IT/IA decision makers select appropriate security solutions for their organizations by focusing on the critical factors contributing to the decision to recommend specific security technologies, particularly the factors that influence IT/IA managers recommendations of biometric security technologies. Specifically, the research can help information technology management professionals determine whether the security effectiveness, organizational need, reliability, and cost/value aspects of biometric security technologies are generally acceptable to IT/IA decision makers. The study can also provide security technology companies with information to assist in the determination of what is important to their customer base when considering the introduction of new IT security products.

A number of researchers have ascribed the rationale for the choice to recommend a new technology to areas of cost-effectiveness, reliability, organizational need, and function-effectiveness (Craig & Hamidi-Noori, 1985; Ettlie, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004).

Following Dynes, Brechbuhl, and Johnson's (2005) findings, the study focused on the principal drivers of organizational adoption of security technology: the perceptions of IT/IA managers and gauged the influence of security effectiveness, need, reliability, and cost-effectiveness on the managers' decisions to recommend biometric security technologies. The conceptual framework for the study was a survey instrument completed by a pool of IT/IA management professionals.



### Research Questions

Drawn from the extant literature and with further development of the relevant concepts, this study investigated the following four research questions. Each of the research questions gauges the respective aspects of IT/IA managers' perceptions of biometrics relative to the following factors identified in the literature: security effectiveness, need, reliability, and cost-effectiveness of biometrics.

Question 1. Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its security effectiveness?

Question 2. Is an IT/IA manager's decision to recommend biometric security technologies independent of his/her perceived need for new security technologies?

Question 3. Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its reliability?

Question 4. Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its cost-effectiveness?

### Research Hypotheses

Based on these research questions, the study tested the research hypotheses listed in Table 4.

Table 4  
*Research Hypotheses*

Hypothesis 1	<p>H01<sub>NULL</sub>: An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its security effectiveness.</p>
	<p>HA1<sub>ALTERNATE</sub>: An IT/IA manager's decision to recommend biometric security technology is dependent on his/her perception of its security effectiveness.</p>
Hypothesis 2	<p>H02<sub>NULL</sub>: An IT/IA manager's decision to recommend biometric security technologies is independent of his/her perceived need for new security technologies.</p>
	<p>HA2<sub>ALTERNATE</sub>: An IT/IA manager's decision to recommend biometric security technologies is dependent on his/her perceived need for new security technologies.</p>
Hypothesis 3	<p>H03<sub>NULL</sub>: An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its reliability.</p>
	<p>HA3<sub>ALTERNATE</sub>: An IT/IA manager's decision to recommend biometric security technology is dependent on his/her perception of its reliability.</p>
Hypothesis 4	<p>H04<sub>NULL</sub>: An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its cost-effectiveness.</p>
	<p>HA4<sub>ALTERNATE</sub>: An IT/IA manager's decision to recommend biometric security technology is dependent on his/her perception of its cost-effectiveness.</p>

### Sample Design

The theoretical study population consisted of all IT/IA professionals in a management role. The study population was IT/IA professionals affiliated with the Northern Virginia Chapter of the Information Systems Security Association (ISSA-NOVA) who volunteered to participate in the study. The assumption was made that IT/IA professionals who are affiliated with ISSA-NOVA and who volunteered to complete online surveys are without significant differences in their attitudes compared to all other IT/IA professionals in the Mid-Atlantic (Maryland, Virginia, and the District of Columbia) area. The sampling frame contained 382 IT/IA professionals on ISSA-NOVA's email directory and represents small, medium, and large-sized organizations. The study did not require that a manager support a particular number of users, but that he/she is familiar with biometric security technologies.

ISSA-NOVA was chartered in 2002 with membership open to IT/IA professionals living within a 100-mile radius of Reston, Virginia, including those with dual membership in the ISSA chapters in Baltimore, Maryland and/or Washington, DC. ISSA-NOVA members are professionals in security management in various sized organizations and industries who choose to network with one another as a forum for technological advice, educational opportunities, vendor and product information, future employment opportunities, and general socialization. The researcher is a member of ISSA-NOVA but holds no office in the organization nor has any undue influence over its officers, employees, or fellow members.

Randomness of the target sample was preserved because each member of the sample had an equal opportunity to complete the survey. Each of the 382 IT/IA professionals on ISSA-NOVA's mailing list was emailed a survey invitation with a link to the survey Web

site in the text in order to minimize sampling error. Additionally, ISSA-NOVA publicized the study by allowing the researcher to announce the study at regularly scheduled monthly meetings, to provide a link to the survey Web site through the ISSA-NOVA Web site ([www.issa-nova.org](http://www.issa-nova.org)), and to publish announcements in the ISSA-NOVA Newsletter.

The survey was hosted by Survey Monkey ([www.surveymonkey.com](http://www.surveymonkey.com)), a professional Web survey hosting company, and available to participants via the Internet. Participants anonymously completed the survey. A limit of only "one response per respondent" was allowed in order to prevent multiple responses. After completing the survey, participants were prevented from entering additional responses. However, participants who did not complete the survey in one visit could return one or more times to complete the survey. After logging in, they were taken to the point that they had previously left off.

The study collected 232 complete surveys, a response rate of 60.7%. This response rate exceeded the minimum number of participants of 156. This minimum sample size was based on Thorndike's (1978) equation for determining adequate sample sizes. The sample size methodology used is the more rigorous of the two methods Thorndike developed. Please see the *Sample and Sample Size Determination* section presented later in this Chapter for an extended discussion of the minimum sample size determination.

### Variables

The specific variables of interest in this study were IT/IA managers' perceived security effectiveness, need, reliability, cost-effectiveness, and decision to recommend biometric security technologies. A number of researchers have ascribed the rationale for the

choice to recommend a new technology to areas of cost-effectiveness, reliability, organizational need, and function-effectiveness (Craig & Hamidi-Noori, 1985; Etlie, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004). Classification and definition of these variables are discussed below.

#### *Dependent Variable*

The dependent variable in this study was the IT/IA manager's willingness to recommend biometric security technologies to his/her organization. Responses to Item 15 measured this variable. Item 15 was, "I would feel comfortable recommending biometric technologies in my organization."

#### *Independent Variables*

The independent variables in this study were the IT/IA manager's perceived security effectiveness, need, reliability, and cost-effectiveness of biometric security technologies.

##### *Security effectiveness*

This independent variable was the IT/IA manager's attitude towards the security of biometric systems. Item 1 measured security effectiveness. Item 1 was, "I feel that biometrics are secure."

##### *Need for biometrics*

This independent variable was the manager's perception that his/her organization needs biometric security technologies to protect its IT assets. Item 8 measured the need for biometrics. Item 8 was, "Biometric technologies would/do provide a significant benefit to my organization."

*Reliability*

This independent variable was the manager's perception of the reliability of biometric security technologies. Item 10 measured reliability. Item 10 was, "Biometric technologies are more reliable than traditional IT security methods."

*Cost-effectiveness*

This independent variable is the manager's perceived level of cost versus benefit for biometric security technologies. Item 12 measured cost-effectiveness. Item 12 was, "Biometric technologies provide a good value for their cost."

*Moderator and Mediator Variables*

Baron and Kenny (1986) distinguish between moderator and mediator variables. They propose the nature of moderator variables as qualitative measures influencing the strength of associations between dependent and independent variables. In contrast, they posit that a mediator variable intervenes between an independent and dependent variable. For example, a computer security training program may intervene between an independent variable (i.e., ease of use) and a dependent variable (i.e., intent to use). There were no intervening processes in this study; therefore, no mediating variables were addressed.

However, it is conceivable that specific demographic characteristics may have an impact on IT/IA managers' willingness to recommend biometric security technologies. Therefore, these characteristics were measured and evaluated for possible impact. In this study, these variables include the following: (a) years of experience implementing biometrics, (b) organization size, (c) title/job function, and (d) industry. Survey Items 17 through 20 measured these variables.

*Other Variables*

Non-response is a potential source of bias in survey studies and must be properly addressed (Fowler, 1993). To mitigate the potential for non-response bias in this study, the researcher compared responses between early and late responders. Early respondents were identified as those respondents who completed the survey within the initial nine-day response window (July 15 through July 23). Late responders were those respondents who completed the survey after the initial nine-day response period (July 24 through August 1).

Another source of bias is the level of activity in the organization. Because the level of activity in organizations can be cyclical, IT/IA managers may have less discretionary time to read and respond to a questionnaire during periods of high activity. It was beyond the scope of this study to ensure that all respondents in the sample population would complete the survey on the same day of the week (or time of day). Therefore, this study did not control the day of the week or the time of day the survey would be completed. Although not investigated, it also is conceivable that the day of the week and/or time of day may introduce some bias into responses to the survey.

Other uncontrolled variables may have included a respondent's bias based on social, emotional, economic, or cultural issues at the time the respondent completed the survey. These variables were not evaluated in this study but may provide opportunities for further research.

### Field/Pilot Trials

As suggested by Cook and Campbell (1979), Nunnally and Bernstein (1994), and Straub (1989), peer review/field trials established the face and content validity of the survey instrument. Peer reviews/field trials to establish validity are appropriate because the survey items represent a defined domain of content and logical validity (Messick, 1998). Two field trials to evaluate the face and content validity of the instrument were completed on April 1, 2005 and June 12, 2005. In accordance with the structure suggested by Yun and Ulrich (2002), the field trials were conducted with ten senior managers in the IT industry who specialize in IA (e.g., information technology security) domains. The purpose of the field trials was to determine the ease of delivering and accessing the survey and if respondents would have difficulty with survey item comprehension and/or the format of the questionnaire.

For both of the field trials, surveys with cover letters were emailed to the ten senior managers. The stated objectives of the field trials were to answer the following questions:

1. Were you able to access the survey without difficulty?
2. Is the content of the questionnaire appropriate for the audience?
3. Are the survey items clear?
4. Do the instructions make sense?
5. Are any of the survey items intrusive, invasive, potentially embarrassing, or of a sensitive nature?
6. Do you have any other comments?



For the April 1, 2005 field trial, subsequent interviews with each of the senior managers revealed some concerns with what they considered redundant survey items. Two of the managers made suggestions to help clarify the survey instructions. The redundant survey items were removed from the survey instrument and the suggested improvements to the instructions were incorporated into the instruments.

For the June 12, 2005 field trial, which used the improved version of the survey instrument and instructions, subsequent interviews with the ten managers supported the ease of access and clarity of the questions and instructions.

### Validity and Reliability

With satisfactory face and content validity established via the field trials and with Institutional Review Board (IRB) approval granted on June 28, 2005, the questionnaire was pre-tested for its reliability (Nunnally & Bernstein, 1994; Straub, 1989).

Reliability was established through a test-retest sequence. The test-retest approach is one of the simplest experimental designs wherein subjects are measured in terms of a dependent variable (the test) and later exposed to a stimulus representing an independent variable (the retest). The differences noted between the first test and the second test are then attributed to the independent variable. The expected outcome of this particular test-retest sequence is that there would be little or no significant difference between the results of Test 1 and Test 2 (Babbie, 2003).

On June 29, 2005, 42 IT Security managers who had previously volunteered to participate in the survey test-retest were invited by email to complete the survey (Test 1). To

ensure that each participant's responses would be reliably matched in both tests, the email invitation included a unique ID code for each participant. This test of the survey instrument yielded 36 complete surveys, a response rate of 86%. Cronbach's alpha was calculated for the 16 Likert-scale survey items and yielded an  $\alpha$  of .94.

Test 2 of the test-retest sequence was completed on July 14. This is within the "two-week to one-month's time in which it is advisable to complete both testings" (p. 40) recommended by Carmines and Zeller (1979), citing Nunnally (1964). There were no changes to the questionnaire between Test 1 and Test 2 and no communication with the respondents, other than to confirm their availability for the re-test and the email invitation itself. As suggested by Carmines and Zeller (1979) and Nunnally and Bernstein (1994), to ensure that Test 2 results were adequately independent of Test 1 results, survey items were randomly ordered. The randomization of the survey items and the time delay between tests are assumed to have adequately mitigated the potential for test-retest bias caused by the participants' memories of their previous responses.

Test 2 yielded 36 complete surveys (a response rate of 100%) with a Cronbach's alpha for the 16 Likert-scale survey items of .94.

#### *Tests for Correlations between Test 1 and Test 2*

As a preliminary step in determining the correlation between Test 1 and Test 2, a scatterplot (Figure 1) was generated to check visually for violation of the assumptions of linearity and homoscedasticity. Interpretation of the scatterplot reveals that the points are neatly arranged along a straight line in a very narrow, nearly cigar shape. Additionally, the

shape of the cluster is almost even from one end to the other. This shape suggests a strong correlation and supports the assumptions of linearity and homoscedasticity.

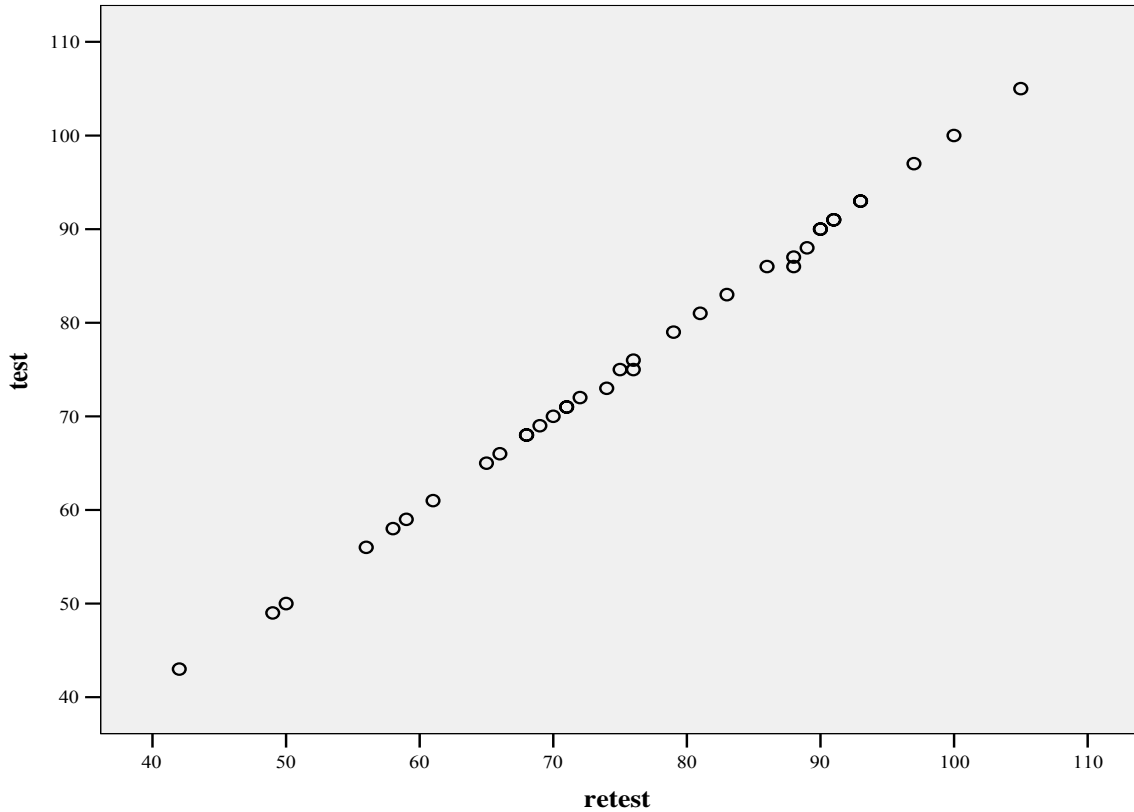


Figure 1. Test-retest scatterplot

With the assumptions of linearity and homoscedasticity confirmed, Pearson's  $r$  is an appropriate measure of the correlation between Test 1 and Test 2. In addition to Pearson's product-moment correlation coefficient, two nonparametric tests of correlation (Kendall's  $\tau_b$  and Spearman's  $\rho$ ) were also performed. Pearson's and Spearman's measures yielded a correlation of identity (1.000) and Kendall's  $\tau_b$  yielded a .997 correlation, with a corresponding .994 coefficient of determination. These results indicate that Test 1 and Test 2 are highly correlated. Tables 5, 6, and 7 present the results of those tests.

Table 5  
*Pearson's r Correlation Coefficients*

		Test	Retest
Test	Pearson Correlation	1	1.000
	Sig. (2-tailed)		.000
	<i>N</i>	36	36
Retest	Pearson Correlation	1.000	1
	Sig. (2-tailed)	.000	
	<i>N</i>	36	36

*Note:* Correlation is significant at the 0.01 level (2-tailed).

Table 6  
*Kendall's tau b Correlation Coefficients*

		Test	Retest	
Kendall's tau b	Test	Correlation Coefficient	1.000	.997
		Sig. (2-tailed)		.000
		<i>N</i>	36	36
	Retest	Correlation Coefficient	.997	1.000
		Sig. (2-tailed)		
		<i>N</i>	36	36

*Note:* Correlation is significant at the 0.01 level (2-tailed).

Table 7  
*Spearman's rho Correlation Coefficients*

		Test	Retest	
Spearman's <i>rho</i>	Test	Correlation Coefficient	1.000	1.000
		Sig. (2-tailed)		.000
		<i>N</i>	36	36
	Retest	Correlation Coefficient	1.000	1.000
		Sig. (2-tailed)		
		<i>N</i>	36	36

*Note:* Correlation is significant at the 0.01 level (2-tailed).

Analysis of the specific survey responses yielded seven observable differences between Test 1 and Test 2. All seven differences were restricted to Items *secure\_2* (“I am/would be concerned with the technology used by the biometric system (e.g., fingerprint verification, facial recognition, hand geometry verification, iris recognition, voice verification)”) and *secure\_5* (“Biometric technologies were not secure three years ago”). Table 8 presents a comparison of Test 1 and Test 2 responses for the seven different responses.

Table 8  
*Comparison of Changed Responses*

Survey Item	Participant Number	Test 1		Test 2		Net Change
		Response	Score	Response	Score	
secure_2	10	Neutral	3	Agree	4	+1
secure_2	25	Neutral	3	Agree	4	+1
secure_2	34	Neutral	3	Agree	4	+1
secure_5	9	Strongly Agree	5	Agree	4	-1
secure_5	24	Neutral	3	Agree	4	+1
secure_5	25	Neutral	3	Agree	4	+1
secure_5	33	Neutral	3	Agree	4	+1

Possible rationale for the changed responses to Items *secure\_2* and *secure\_5* include the possibility that survey participants changed their attitudes towards certain aspects of biometric security over time, the possibility of human error (the participant selected an unintended response), and the possibility that Items *secure\_2* and *secure\_5* reflect more controversial, complex, or ambiguous constructs. Therefore, the changed responses reflect a greater degree of uncertainty on the part of the survey participant.

#### Minimum Sample Size Determination

To perform a meaningful assessment of an association between the one dependent and four independent variables within this population, it is important to limit the number of moderating variables and acknowledge each moderator used. This study differentiated the

following four moderating variables: (a) years of experience with biometrics, (b) organization size, (c) title/job function, and (d) industry. Therefore, this study was conducted using a total of nine variables.

The literature offered a number of determinants of sample size (Barcikowski & Stevens, 1975; Kish, 1965; Leahy, 1988; Madansky, 1990; Moreno-Robello, 1999; Noether, 1987; Thorndike, 1978). Thorndike's (1978) methods for calculating the minimum acceptable response were appropriate for this study.

According to Thorndike (1978), an association of direct proportion exists between the sample size and the total number of variables. He suggests an informal approach of ten responses per variable plus a modifier of 50 to be added in order to assure reliability when sample sizes are small. Expressed as an equation, this approach yields the following:

$$N \geq (10 \times V) + 50$$

in which  $N$  is the minimum acceptable number responses and  $V$  is the number of variables in a study.

Thorndike (1978) also proposed a more rigorous method, in which  $N$  is a function of the square of the number of variables plus a modifier of 50 to 100 to be added in order to assure reliability when sample sizes are small. Expressed as an equation, this approach yields the following:

$$N \geq V^2 + 50$$

in which  $N$  is the minimum acceptable number responses and  $V$  is the number of variables used in a study. In this case, the minimum acceptable sample size increases at an exponential rate as the number of variables rise. Thorndike's rationale for this method relies on his

observation that the number of correlations between variables increases at a rate faster than the concomitant increase in the number of variables.

Using Thorndike's (1978) methodology for this study (nine variables and a small sample modifier of 75) invokes minimum responses of the following magnitude:

$$156 = 9^2 + 75$$

Seventy-five was the selected modifier value in this instance because it is the mid-point between Thorndike's (1978) range of 50 to 100 as moderator values.

### Survey Instrument

The data for this study was collected via Web-based questionnaire. The questionnaire was field tested to verify content validity and reliability. Please refer to the *Field/Pilot Trials* section presented earlier in this chapter for more information on the field trials.

### Data Collection

Data was collected by a survey questionnaire administered by the researcher on the Internet. Survey respondents were recruited through an email invitation sent to 382 IT/IA professionals on ISSA-NOVA's mailing list, announcements posted in the ISSA-NOVA newsletter and on the ISSA-NOVA Web site ([www.issa-nova.org](http://www.issa-nova.org)), and personal announcements/reminders by the researcher at monthly ISSA-NOVA meetings. Inducements included a copy of a report written by the researcher (*Enhancing Security in the Private Sector with Biometric Technology: Problems and Prospects*), a copy of the research results, and the researcher's words of heartfelt gratitude.



The active membership of ISSA-NOVA is approximately 400 IT/IA professionals. On average, 100 to 150 members attend the monthly meetings with about half that number comprised of regulars, members who attend nine or more meetings each year, and drop-ins, members who attend three or fewer meetings each year. The researcher had adequate time during each meeting to recruit survey respondents. Additionally, at the April 19, 2005 and May 19, 2005 meetings, an informal indicator of interest revealed that 78 and 103 (respectively) members attending the meetings were interested in completing the questionnaire, provided they could receive a copy of the results.

The survey site Web address was distributed via email by ISSA-NOVA to 382 IT and IA managers and executives representing primarily the Mid Atlantic (Maryland, Virginia, and the District of Columbia) area of the U.S. Each survey participant was provided with instructions for the survey, the informed consent form, and assurances of confidentiality.

Figures 2a, 2b, 3a, and 3b present the content of the survey instrument and demographic questionnaire for use in this research effort. The survey items consisted of 16 semantic differential items arranged in a Likert (1932) format and four multiple-choice demographic questions.

The survey instrument was organized into six sections. The first section of the instrument (Items 1 through 5) relates to IT/IA managers' perceptions of the security effectiveness of biometrics. Section 2 (Items 6 through 8) relates to perceptions of need for biometric security technologies. Section 3 (Items 9 through 11) relates to the managers' perceptions of the reliability of biometrics. The fourth section (Items 12 through 14) relates to IT/IA managers' attitudes toward the cost-effectiveness of biometrics. Section 5 of the

biometrics survey instrument (Items 15 and 16) gains an understanding of the participants' perceptions of the technology overall. A five-point Likert (1932) semantic differential scale (*strongly disagree* = 1 to *strongly agree* = 5) was used for sections one through five. The final section of the survey instrument identified survey participant demographics and asked multiple-choice questions regarding the participants' years of experience with biometrics, organization size, title/job function, and industry.

Please note that Figures 2a, 2b, 3a, and 3b do not present the survey instruments exactly as they appeared on the Survey Monkey survey site.

Item No.	Below are 16 statements about biometric security technologies. Please indicate if you agree or disagree with each statement by selecting the appropriate number on the scale of 1 (strongly disagree) to 5 (strongly agree) that most closely matches your perception of biometric security technologies. When you are satisfied with your answers, please click the “CONTINUE” button to proceed to the final section of the survey.	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	I feel that biometrics are secure.	1	2	3	4	5
2	I am/would be concerned with the technology used by the biometric system (e.g., fingerprint verification, facial recognition, hand geometry verification, iris recognition, voice verification).	1	2	3	4	5
3	I feel that biometric technologies are more secure than traditional IT security methods.	1	2	3	4	5
4	I am willing to use biometric technologies to protect sensitive information at my organization.	1	2	3	4	5
5	Biometric technologies were not secure three years ago.	1	2	3	4	5
6	My organization needs to improve the security of its IT assets.	1	2	3	4	5
7	My organization needs biometric technologies to secure its IT assets.	1	2	3	4	5
8	Biometric technologies would/do provide a significant benefit to my organization.	1	2	3	4	5
9	Biometric technologies are inherently reliable.	1	2	3	4	5
10	Biometric technologies are more reliable than traditional IT security methods	1	2	3	4	5
11	Biometric hardware is reliable.	1	2	3	4	5
12	Biometric technologies provide a good value for their costs.	1	2	3	4	5

Figure 2a. Biometrics data collection instrument

Item No.		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
13	The cost of maintenance is lower with biometric technologies than with traditional IT security methods.	1	2	3	4	5
14	I would consider biometric technologies to have considerable cost savings over traditional IT security methods.	1	2	3	4	5
15	I would feel comfortable recommending biometric technologies in my organization.	1	2	3	4	5
16	I feel that biometric systems use proven technology.	1	2	3	4	5

Figure 2b. Biometrics data collection instrument

17.	How many years of experience do you have implementing biometric security technologies?	None	<input type="checkbox"/>
		Less than 2 years	<input type="checkbox"/>
		Two years to less than 5 years	<input type="checkbox"/>
		Five years or more	<input type="checkbox"/>
18.	How many users does your organization support?	Less than 50 users	<input type="checkbox"/>
		Fifty users to less than 1,000 users	<input type="checkbox"/>
		1,000 users to less than 5,000 users	<input type="checkbox"/>
		5,000 users or more	<input type="checkbox"/>
19.	What best describes your title?	Information Technology (IT) Manager	<input type="checkbox"/>
		Information Assurance (IA) Manager	<input type="checkbox"/>
		IT Director	<input type="checkbox"/>
		IA Director	<input type="checkbox"/>
		Vice President of IT	<input type="checkbox"/>
		Vice President of IA	<input type="checkbox"/>
		Chief Technology Officer (CTO)	<input type="checkbox"/>
		Chief Information Officer (CIO)	<input type="checkbox"/>
		Chief Security Officer (CSO)	<input type="checkbox"/>
		Other IT	<input type="checkbox"/>
		Other IA	<input type="checkbox"/>
None of the above	<input type="checkbox"/>		

Figure 3a. Demographics data collection instrument

20.	What is the primary business or industry of your organization?	Construction	<input type="checkbox"/>
		Education	<input type="checkbox"/>
		Energy/Utilities	<input type="checkbox"/>
		Financial Services/Banking	<input type="checkbox"/>
		Government	<input type="checkbox"/>
		Health Care	<input type="checkbox"/>
		Information Technology – Manufacturing	<input type="checkbox"/>
		Information Technology – Services	<input type="checkbox"/>
		Manufacturing (non-IT)	<input type="checkbox"/>
		Professional, Technical, and Business Services (non-IT)	<input type="checkbox"/>
		Real Estate	<input type="checkbox"/>
		Retail	<input type="checkbox"/>
		Telecommunications	<input type="checkbox"/>
		Travel/Leisure/Hospitality	<input type="checkbox"/>
		Wholesale Distribution and Services	<input type="checkbox"/>
Other	<input type="checkbox"/>		

Figure 3b. Demographics data collection instrument

### Data Confidentiality

The study did not collect any personally identifiable information. Nevertheless, the data was handled in a manner consistent with sound practices for safeguarding personal data. Survey data was initially maintained on magnetic media on Survey Monkey’s server. At the completion of the data collection phase of the study, the survey results were downloaded from the server to the researcher’s workstation. The researcher confirmed that the data was

readable/not corrupted and notified Survey Monkey to delete permanently the data from the server.

The researcher has retained copies of all dissertation-related information, including survey data, on a CD-ROM secured within the researcher's safety deposit box. The data may be destroyed after seven years.

### Data Analysis

For hypothesis testing and descriptive statistics, Statistical Package for Social Science (SPSS) Version 13.0 was used. Each of the four hypotheses was tested using the Chi Square Test of Independence. The significance level was set at 0.05. Table 9 presents a summary of the variables collected and analyzed in this study.

Table 9  
*Data Collection and Analysis Summary*

Category	Variable	How Measured	Scale and Values
Dependent	Decision to recommend biometrics	Analysis of: Independence (Chi Square) Nonresponse (late response) bias	
Independent	Security effectiveness	Semantic differential	Five-point Likert
Independent	Need for biometrics	Semantic differential	Five-point Likert
Independent	Reliability	Semantic differential	Five-point Likert
Independent	Cost-effectiveness	Semantic differential	Five-point Likert
Moderator	Experience	Interval	1 to 4
Moderator	Organization size	Interval	1 to 4
Moderator	Job function/title	Nominal	1 of 12
Moderator	Industry	Nominal	1 of 16

*Data Coding*

For the first 16 items, a *strongly agree* was the only response that equated to a fully committed recommendation. The responses, therefore, were coded into two possible categories: *strongly agree* (coded as 1) and *less than strongly agree* (coded as 2). Figures 4a, 4b, 5a, and 5b present the data coding protocol for the biometric security technology items and the demographic questions (respectively).

Q#	Security Effectiveness	Code
1	I feel that biometrics are secure.	S1
2	I am/would be concerned with the technology used by the biometric system (e.g., fingerprint verification, facial recognition, hand geometry verification, iris recognition, voice verification).	S2
3	I feel that biometric technologies are more secure than traditional IT security methods.	S2
4	I am willing to use biometric technologies to protect sensitive information at my organization.	S2
5	Biometric technologies were not secure three years ago.	S2
	Need for Biometrics	
6	My organization needs to improve the security of its IT assets.	N2
7	My organization needs biometric technologies to secure its IT assets.	N1
8	Biometric technologies would/do provide a significant benefit to my organization.	N2
	Reliability	
9	Biometric technologies are inherently reliable.	R1
10	Biometric technologies are more reliable than traditional IT security methods	R2
11	Biometric hardware is reliable.	R2

Figure 4a. Biometric item coding protocol



Cost-Effectiveness		
12	Biometric technologies provide a good value for their costs.	C1
13	The cost of maintenance is lower with biometric technologies than with traditional IT security methods.	C2
14	I would consider biometric technologies to have considerable cost savings over traditional IT security methods.	C2
Decision to Recommend		
15	I would feel comfortable recommending biometric technologies in my organization.	D1
16	I feel that biometric systems use proven technology.	D2

Figure 4b. Biometric item coding protocol

Q#	Question	Value	Code
17	How many years of experience do you have implementing biometric security technologies?	None	E1
		Less than 2 years	E2
		Two years to less than 5 years	E3
		Five years or more	E4
18	How many users does your organization support?	Less than 50 users	U1
		Fifty users to less than 1,000 users	U2
		1,000 users to less than 5,000 users	U3
		5,000 users or more	U4
19	What best describes your title?	Information Technology (IT) Manager	T1
		Information Assurance (IA) Manager	T2
		IT Director	T3
		IA Director	T4
		Vice President of IT	T5
		Vice President of IA	T6
		Chief Technology Officer (CTO)	T7
		Chief Information Officer (CIO)	T8
		Chief Security Officer (CSO)	T9
		Other IT	T10
		Other IA	T11
		None of the above	T12

Figure 5a. Demographic information coding protocol

20.	What is the primary business or industry of your organization?	Construction	B1
		Education	B2
		Energy/Utilities	B3
		Financial Services/Banking	B4
		Government	B5
		Health Care	B6
		Information Technology – Manufacturing	B7
		Information Technology – Services	B8
		Manufacturing (non-IT)	B9
		Professional, Technical, and Business Services (non-IT)	B10
		Real Estate	B11
		Retail	B12
		Telecommunications	B13
		Travel/Leisure/Hospitality	B14
		Wholesale Distribution and Services	B15
		Other	B16

Figure 5b. Demographic information coding protocol

*Treatment of Missing Data*

Norusis (2005) and Babbie (2003) provide the following framework for the treatment of missing data:

1. Missing responses for a specific survey item can be excluded if the number of usable responses is adequate for valid indexing and statistical analysis.
  2. The researcher may arbitrarily assign a default value to missing data.
  3. A value can be assigned after a "careful analysis and interpretation of missing data"
- (Babbie, 2003, p. 172).

There were no incomplete responses or missing data for this study.

### Potential Limitations of the Study Methodology

The principal limitation of the study is the limited generalizability of the results due to the sample. It is likely that the research results from the sample of 382 IT/IA professionals in the Mid-Atlantic (Maryland, Virginia, and District of Columbia) area present limited potential for generalization to the population of IT/IA professionals.

Additionally, external validity can be threatened by several error-types including a desire by the respondent to impress the researcher or to emphasize a preference by scoring survey items at either extreme of the scale. Surveys measuring responses to issues perceived as highly controversial or intimate are often susceptible to respondent bias. Survey items perceived as relatively neutral, however, do not threaten external validity. This survey was an anonymous measure of attitudes towards technology and, therefore, mitigated the probability of respondent bias.

As with any voluntary survey, the potential for non-response bias always exists. Members of the sample may choose not to respond to the survey for a variety of reasons including a lack of motivation or interest, too busy, or other personal and/or work-related reasons. Furthermore, survey respondents may choose not to answer one or more survey items for a number of reasons, including the following: (a) the item is not relevant to their particular situation, (b) the options available to the respondent do not represent the respondent's true attitude or opinions, (c) the respondent does not understand the meaning of the survey item, or (d) completion of the item may embarrass the respondent or bring him/her discomfort (Erdos, 1970; Mangione, 1995). Item non-response results in incomplete data that

can adversely impact the reliability of the findings. For this survey instrument, there were no responses with missing values.

To mitigate the potential of non-response, the researcher provided presentations at the monthly ISSA-NOVA meetings and offered copies of the results of the survey and copies of the researcher's report, *Enhancing Security in the Private Sector with Biometric Technology: Problems and Prospects*, to all respondents who requested one or both of the reports.

Another potential limitation is that respondents may be concerned with risks associated with replying to a survey that relates to their jobs. To alleviate this concern, the researcher included statements that assured confidentiality to each respondent and told the respondents that the survey results would not include identifying data about them or their organizations.

## CHAPTER 4. DATA COLLECTION AND ANALYSIS

This chapter reports responses, data analysis, and study findings. The purpose of the study was to help information technology and information assurance (IT/IA) decision makers select appropriate security solutions for their organizations by focusing on the critical factors contributing to the decision to recommend specific security technologies, in particular the factors that influenced IT/IA managers to recommend biometric security technologies. Specifically, the research can help information technology management professionals determine whether the security effectiveness, organizational need, reliability, and cost/value aspects of biometric security technologies are generally acceptable to IT/IA decision makers. The study can also provide security technology companies with information to assist in the determination of what is important to their customer base when considering the introduction of new IT security products.

### Data Collection, Response Rates, and Population

Survey invitations were sent by email to 382 members of ISSA-NOVA, a chapter of the International Systems Security Association (ISSA), which is a professional association of IT and IA managers and practitioners. ISSA-NOVA's members are located primarily in the Mid-Atlantic (Maryland, Virginia, and District of Columbia) area. The survey was available to all 382 members of ISSA-NOVA from July 15, 2005 to August 1, 2005. During this period, 232 surveys were completed with a response rate of 60.7% of the membership population. It is assumed that the survey results are reasonably representative of the

population of IT and IA managers in the Mid-Atlantic area because ISSA-NOVA members include IT and IA professionals from various sized companies in a wide range of industries.

The survey responses were downloaded by the researcher and exported into SPSS 13 for analysis. Outlier detection was conducted and data entry errors were corrected.

Additionally, a positive (albeit small) correlation was validated between early responses (July 15 through July 23) and late responses (July 24 through August 1). Reliability was also re-validated through the use of Cronbach's alpha, with a resulting alpha of 0.89.

### Demographic Characteristics of the Sample

The survey included questions that were gathered for further research. The focus of the study was to determine what factors influence managers' decisions to recommend or not to recommend biometric security technology regardless of their previous experience, organization size, title/job function, or industry. The suggestions for further research section in Chapter 5 address the possibility of reexamining the data to determine what, if any, influence demographics may have on the results of the survey.

#### *Summary Representation of the Sample*

A majority (61.6%) of the respondents reported five or more years of experience in implementing biometric security technologies. Over one half (52.2%) of the respondents' organizations were large and supported 5,000 users or more. The titles/job functions reported by the respondents were widely distributed from 22.6% (Other IT) to 0.4% (Vice President of Information Assurance). Industry groups were also widely distributed from 36.6% reporting Information Technology – Services, to 0.4% reporting Travel/Leisure/Hospitality or

Wholesale Distribution and Services. The following sections discuss the sample demographics of previous experience, organization size, titles/job functions, and industries in greater detail.

#### *Previous Experience*

The survey respondents were similar with regard to their years of experience in implementing biometric security technologies. Approximately 94% of the respondents had experience implementing biometrics – with nearly two-thirds having five years or more of biometrics experience. Refer to Table 10 and Figure 5 for the experience frequency distribution.

Table 10  
*Previous Experience Frequency Distribution*

Previous Experience	Frequency	Percent	Cumulative Percent
None	14	6.0	6.0
Less than two years	39	16.8	22.8
Two years to less than five years	36	15.5	38.4
Five years or more	143	61.6	100.0
Totals	232	100.0	

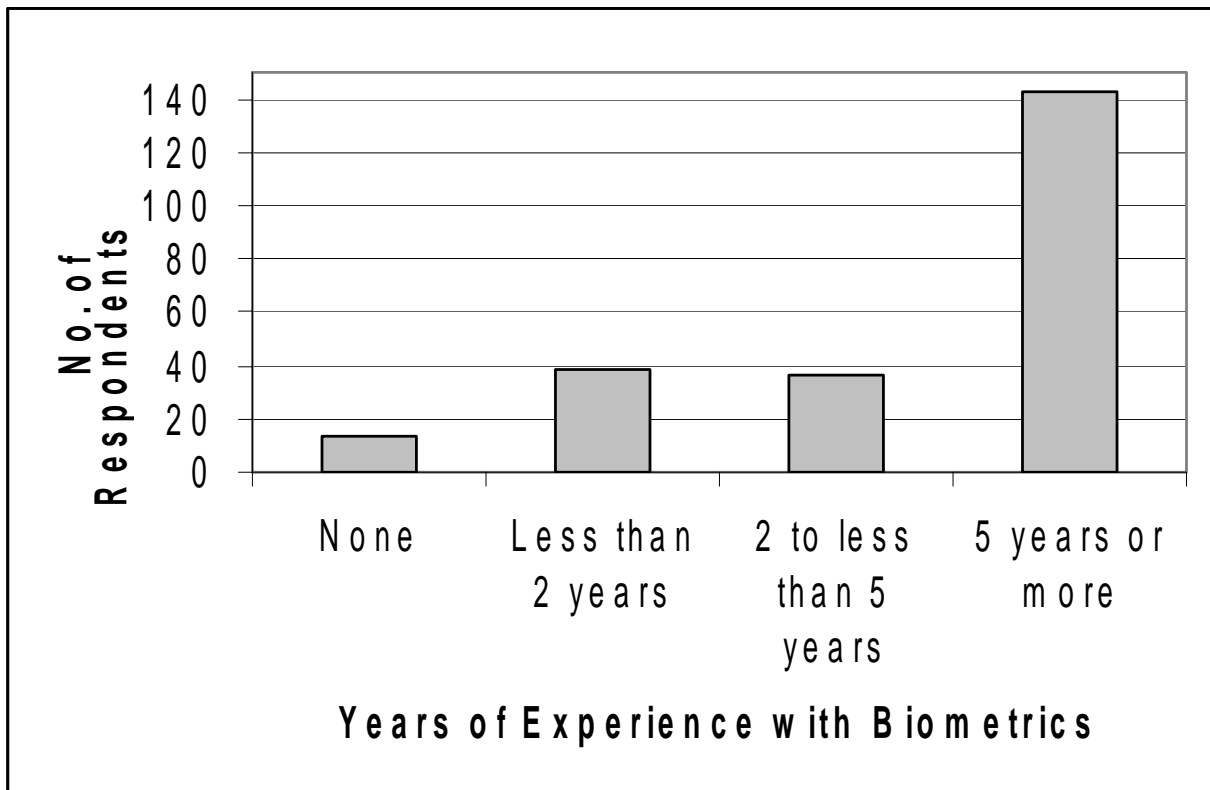


Figure 6. Distribution of previous experience

Crosstabulation analysis of the managers' years of experience and their willingness to recommend biometric security technology provided results indicating that as experience increased, managers were more likely to *strongly agree* that they would be comfortable recommending biometric security technologies. Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*. Refer to Table 11 for the crosstabulation analysis.



Table 11  
*Previous Experience and Recommendation Crosstabulation*

Years of Experience with Biometrics	I would recommend biometric technologies in my organization		Totals
	Strongly Agree	Less than Strongly Agree	
None	0 (0.0)	14 (100)	14 (100)
Less than two years	3 (7.7)	36 (92.3)	39 (100)
Two years to less than five years	4 (11.1)	32 (88.9)	36 (100)
Five years or more	26 (18.3)	117 (81.8)	143 (100)
Totals	33	199	232

*Note:* Numbers in parentheses indicate percent of the total in each category.

#### *Organization Size*

Survey respondents' employment tended toward larger organizations with over half of the respondents reporting that they support 5,000 users or more. Conversely, only 8.2 percent of the respondents reported supporting organizations with 50 or fewer users. Table 12 and Figure 6 provide the organization size frequency distribution.

Table 12  
*Organization Size Frequency Distribution*

Number of Users	Frequency	Percent	Cumulative Percent
Less than fifty users	19	8.2	8.2
Fifty users to less than 1,000 users	54	23.2	31.5
1,000 users to less than 5,000 users	38	16.4	47.8
5,000 users or more	121	52.2	100.0
Totals	232	100.0	

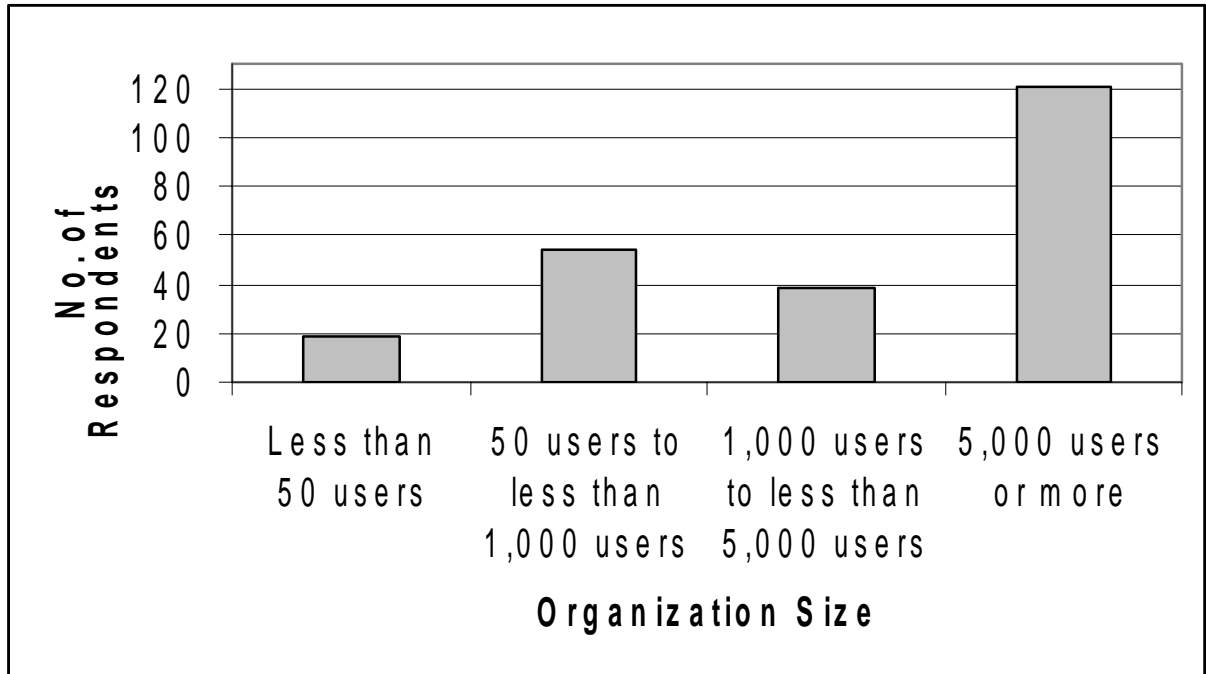


Figure 7. Distribution of organization size

Crosstabulation analysis of the number of users the managers support and their willingness to recommend biometric security technology provided results indicating that those managers supporting mid-size to large organizations (50 users to less than 5,000 users) were more likely to recommend biometric security technologies than those supporting either very small or very large organizations. Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*. Refer to Table 13 for the crosstabulation analysis.

Table 13  
*Organization Size and Recommendation Crosstabulation*

Number of Users	I would recommend biometric technologies in my organization		Totals
	Strongly Agree	Less than Strongly Agree	
Less than fifty users	0 (0.0)	19 (100)	19 (100)
Fifty users to less than 1,000 users	5 (9.3)	49 (90.7)	54 (100)
1,000 users to less than 5,000 users	20 (52.6)	18 (47.4)	38 (100)
5,000 users or more	8 (6.6)	113 (93.4)	121 (100)
Totals	33	199	232

*Note:* Numbers in parentheses indicate percent of the total in each category.

#### *Titles/Job Functions*

The survey respondents were divided in their reported titles/job functions. From the researcher's experience, the distribution of titles/job functions in the sample is reasonably consistent with the distribution found in the general population. Organizations usually have fewer vice presidents and other senior executives than directors, fewer directors than managers, and fewer managers than other employees. Table 14 and Figure 7 provide the frequency distribution of the respondents' titles/job functions.

Table 14  
*Title/Job Function Frequency Distribution*

Title/Job Function	Frequency	Percent	Cumulative Percent
Other IT	53	22.9	22.9
IT Director	48	20.7	43.6
IT Manager	38	16.4	60.0
IA Manager	25	10.8	70.8
IA Director	21	9.1	79.9
Chief Information Officer	14	6.0	85.9
Chief Security Officer	11	4.7	90.6
Other IA	10	4.3	94.9
Chief Technology Officer	4	1.7	96.6
Vice President of IT	4	1.7	98.3
None of the above	3	1.3	99.6
Vice President of IA	1	0.4	100.0
Totals	232	100.0	

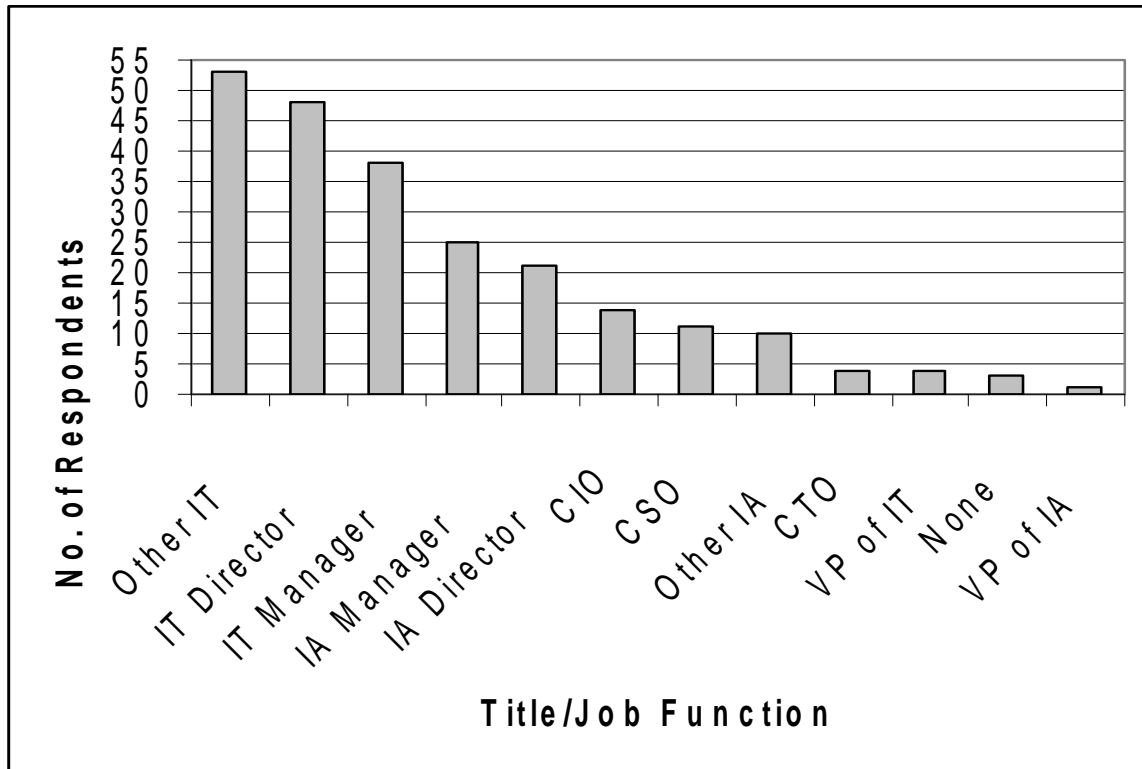


Figure 8. Distribution of title/job functions

A crosstabulation by title/job function and recommendation shows that the respondents were divided in their willingness to recommend biometric security technologies. No significant majority of respondents in any one title/job function *strongly agreed* that they would recommend biometric security technologies. Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*. Table 15 displays the results of this analysis.

Table 15  
*Title/Job Function and Recommendation Crosstabulation*

Title/Job Function	I would recommend biometric technologies in my organization		Totals
	Strongly Agree	Less than Strongly Agree	
Other IT	11 (20.8)	42 (79.2)	53 (100)
IT Director	4 (8.3)	44 (91.7)	48 (100)
IT Manager	4 (10.5)	34 (89.5)	38 (100)
IA Manager	3 (12.0)	22 (88.0)	25 (100)
IA Director	4 (19.0)	17 (81.0)	21 (100)
Chief Information Officer	3 (21.4)	11 (78.6)	14 (100)
Chief Security Officer	1 (9.1)	10 (90.9)	11 (100)
Other IA	1 (10.0)	9 (90.0)	10 (100)
Chief Technology Officer	0 (0.0)	4 (100)	4 (100)
Vice President of IT	0 (0.0)	4 (100)	4 (100)
None of the above	1 (33.3)	2 (66.7)	3 (100)
Vice President of IA	1 (100)	0 (0.0)	1 (100)
Totals	33	199	232

*Note:* Numbers in parentheses indicate percent of the total in each category.

*Industries*

The survey respondents were divided in their reported industries. Information Technology – Services and Government were the two largest industry sectors accounting for 56.4 percent of the responses. Table 16 and Figure 8 provide the frequency distribution of the respondents' industries.

Table 16  
*Industry Frequency Distribution*

Industry	Frequency	Percent	Cumulative Percent
Information Technology – Services	85	36.6	36.6
Government	46	19.8	56.4
Education	22	9.5	65.9
Telecommunications	19	8.2	74.1
Financial Services/Banking	15	6.5	80.6
Professional, Technical, and Business Services (non-IT)	14	6.0	86.6
Health Care	12	5.2	91.8
Manufacturing (non-IT)	9	3.9	95.7
Retail	5	2.2	97.9
Information Technology – Manufacturing	3	1.3	99.2
Travel/Leisure/Hospitality	1	0.4	99.6
Wholesale Distribution and Services	1	0.4	100.0
Totals	232	100.0	

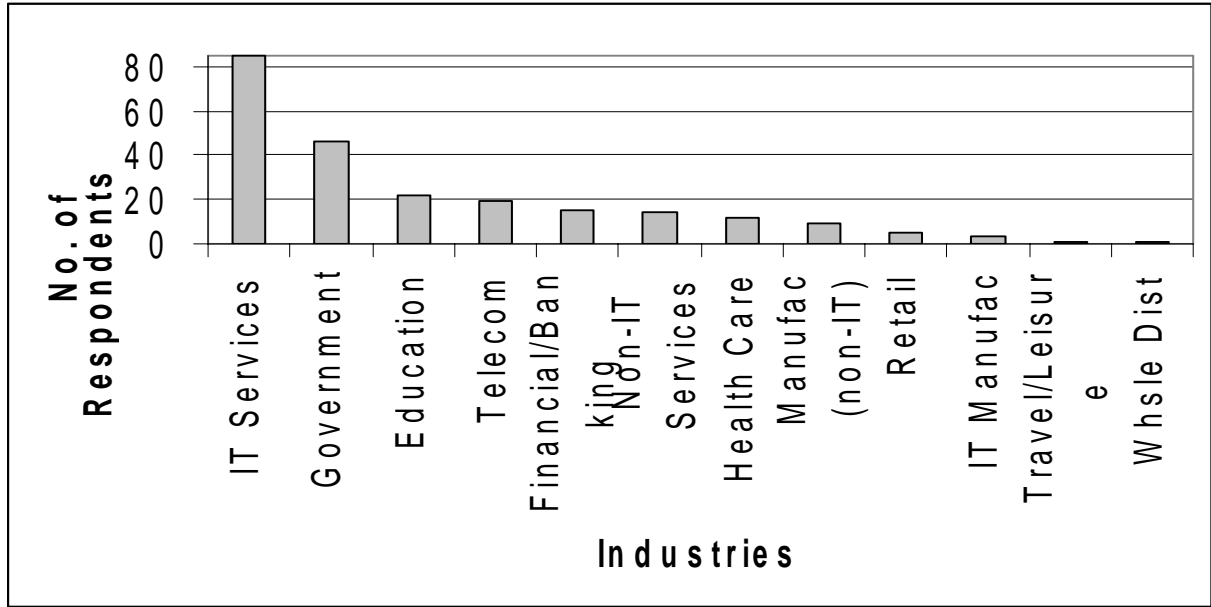


Figure 9. Distribution of industries

A crosstabulation by industry and recommendation shows that the respondents were divided in their willingness to recommend biometric security technologies. No significant majority of respondents in any one industry *strongly agreed* that they would recommend biometric security technologies. Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*. Table 17 displays the results of this analysis.



Table 17  
*Industry and Recommendation Crosstabulation*

Industry	I would recommend biometric technologies in my organization		Totals
	Strongly Agree	Less than Strongly Agree	
Information Technology – Services	11 (12.9)	74 (87.1)	85 (100)
Government	2 (4.3)	44 (95.7)	46 (100)
Education	0 (0.0)	22 (100)	22 (100)
Telecommunications	5 (26.3)	14 (73.7)	19 (100)
Financial Services/Banking	4 (26.7)	11 (73.3)	15 (100)
Professional, Technical, and Business Services (non-IT)	3 (21.4)	11 (78.6)	14 (100)
Health Care	6 (50.0)	6 (50.0)	12 (100)
Manufacturing (non-IT)	0 (0.0)	9 (100)	9 (100)
Retail	0 (0.0)	5 (100)	5 (100)
Information Technology – Manufacturing	1 (33.3)	2 (66.7)	3 (100)
Travel/Leisure/Hospitality	0 (0.0)	1 (100)	1 (100)
Wholesale Distribution and Services	1 (100)	0 (0.0)	1 (100)
Totals	33	199	232

*Note:* Numbers in parentheses indicate percent of the total in each category.

## Descriptive Statistics

The item means and standard deviations are presented in Table 18. On a five-point scale, where 1 = *strongly disagree* to 5 = *strongly agree*, the means ranged from 2.73 (Item 14, “I would consider biometric technologies to have significant cost savings over traditional IT security methods”) to 4.29 (Item 6, “My organization needs to improve the security of its IT assets”). Standard deviations ranged from .60 (Item 6, “My organization needs to improve the security of its IT assets”) to .82 (Item 10, “Biometric technologies are more reliable than traditional IT security methods”).

Table 18  
*Means and Standard Deviations*

Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Mean	3.9	3.8	4.0	4.00	3.0	4.3	3.6	3.8	3.3	3.8	3.7	3.2	3.1	2.7	3.8	3.8
Standard Deviation	.72	.77	.81	.66	.75	.60	.74	.73	.81	.82	.76	.78	.78	.78	.75	.71

The inter-item correlations are presented in Table 19. Examination of the correlation matrix indicated that all items correlated  $\geq |.30|$  with at least three other survey items in the matrix (range: 3 – 13). Eleven of the 16 items (68%) had nine or more shared correlations  $\geq |.30|$ . No inter-item correlation exceeded  $r = .90$ , indicating few problems with multicollinearity (Tabachnick & Fidell, 2001).

Table 19  
*Inter-Item Correlation Matrix*

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1.0															
2	.25	1.0														
3	.86	.22	1.0													
4	.78	.10	.70	1.0												
5	-.45	-.01	-.40	-.43	1.0											
6	.38	.07	.42	.36	-.09	1.0										
7	.59	.07	.61	.46	-.49	.07	1.0									
8	.80	.34	.73	.68	-.40	.29	.71	1.0								
9	.18	-.11	.16	.32	-.04	-.00	-.03	.22	1.0							
10	.77	.19	.77	.68	-.44	.18	.65	.78	.40	1.0						
11	.67	.25	.65	.56	-.36	.06	.55	.77	.41	.89	1.0					
12	.60	.11	.55	.61	-.20	.39	.28	.60	.62	.68	.63	1.0				
13	.25	.20	.23	.19	.01	-.02	.03	.36	.66	.47	.51	.59	1.0			
14	-.02	-.21	-.07	.03	.17	-.27	.03	.02	.58	.18	.14	.34	.61	1.0		
15	.87	.33	.80	.81	-.41	.33	.69	.89	.24	.83	.76	.64	.30	.04	1.0	
16	.70	.35	.69	.56	-.35	.17	.55	.75	.35	.84	.87	.58	.44	.08	.78	1.0

### Exploratory Factor Analysis

Bartlett's test of sphericity and the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy were used to evaluate the strength of the linear association among the 16 survey items in the correlation matrix. Bartlett's test of sphericity was significant ( $\chi^2 = 3723.691, p$

= .001), which indicated that the correlation matrix was not an identity matrix. The KMO statistic (.86), which is an index that compares the magnitude of the observed correlations to the magnitude of the partial correlation coefficients, was mid-way between “marvelous” and “meritorious” according to Kaiser’s (1974) criteria. These results suggested that a factor analysis was appropriate and could be expected to yield common factors.

Among the many factor extraction techniques available to the researcher, Pett, Lackey, and Sullivan (2003) suggest principal components analysis (PCA) for exploratory factor analysis. Additionally, PCA appears to be a good choice because it is relatively immune to multicollinearity issues (Tabachnick & Fidell, 2001). In light of the use of PCA, from this point forward, this dissertation uses the word “component” interchangeably with the word “factor.” Having determined the suitability of factor analysis and an appropriate technique, the next step was to select the number of components/factors to retain.

#### *Selection of the Number of Components/Factors to Retain*

The first task in the component extraction process was to determine the number of initial components that appear to represent the principal dimensions of a manager’s willingness to recommend biometric security technologies in his/her organization. The goal of reducing the number of components from the initial 16 to some lesser number was to explain the amount of total variance with the least number of components. Although there is no one approach to determining the number of components to retain, there are several guidelines that can be used to help determine the number of components to retain. Table 20 presents a summary of the approaches used in selecting the number of factors to retain.

Table 20  
*Selection of the Number of Factors to Retain*

Approach	Number of Factors
Eigenvalues > 1	4
Percent of Variance Extracted (75% to 80%)	4
Examination of Scree Plot	2 to 4

Based on the data in Table 20, four initial components were selected for retention. With the number of components to retain selected, the analysis focused on the total variance explained by each component, component intercorrelations, item loadings on each component, and a determination of the stability of each component. The following sections discuss the analysis and findings.

#### *Total Variance Explained*

Table 21 presents the total variance explained by each component. As mentioned earlier, the extraction method used was PCA. The rotation method was Direct Oblimin with Kaiser Normalization. Oblique rotation via Direct Oblimin was selected because there is a reasonable assumption in social science research that the components possess some degree of correlation, despite being conceptually different (Pett, Lackey, & Sullivan, 2003; Pedhazur & Schmelkin, 1991). Consequently, orthogonal solutions may be “in most instances, naïve, unrealistic portrayals of sociobehavioral phenomena” (Pedhazur & Schmelkin, 1991, p. 615).

Table 21  
*Total Variance Explained*

Component	Rotation Sums of Squared Loadings
	Total
1	8.020
2	2.482
3	1.251
4	1.202

*Note:* When components are correlated, sums of squared loadings cannot be added together to obtain a total variance.

As shown in Table 21, Component 1 accounts for the lion's share of total variance with significantly less total variance explained by Components 2 through 4.

*Component Intercorrelations*

Table 22 presents the component correlation matrix. The component correlation matrix is a matrix of intercorrelations among the components. The data in Table 13 suggests that there is little to no intercorrelations between the components.

Table 22  
*Component Correlation Matrix*

Component	1	2	3	4
1	1.000	.000	-.003	-.013
2	.000	1.000	.014	.018
3	-.003	.014	1.000	.022
4	-.013	.018	.022	1.000

*Rotated Solutions*

Tables 23a and 23b present the rotated component pattern matrix showing all loadings on the initial four components. The component pattern matrix loadings indicate the effect of a given component on a given survey item while controlling for other components. The loadings are similar to partial standardized regression coefficients in a multiple regression analysis (Pett, Lackey, & Sullivan, 2003).

Table 23a  
*Rotated Component Pattern Matrix*

Item	Component			
	1	2	3	4
I would recommend biometric technologies in my organization	.937	-.144	.016	.046
Biometric technologies are more reliable than traditional IT security methods	.929	.086	-.138	-.020
Biometric technologies provide a significant benefit to my organization	.900	-.127	-.062	.113
I feel that biometrics are secure	.889	-.210	.110	-.032
Biometric hardware is reliable	.869	.145	-.227	.143
I feel that biometric systems use proven technology	.865	.046	-.148	.217
Biometric technologies are more secure than traditional IT security methods	.851	-.239	.130	-.035
I am willing to use biometric technologies to protect sensitive information at my organization	.795	-.109	.217	-.227
Biometric technologies provide a good value for their cost	.754	.379	.351	-.056
My organization needs biometric technologies to secure its IT assets	.678	-.295	-.413	-.202

Table 23b  
*Rotated Component Pattern Matrix*

Item	Component			
	1	2	3	4
Biometric technologies were not secure three years ago	-.476	.322	.268	.378
Biometric technologies have considerable cost savings over traditional IT security methods	.125	.834	-.152	-.183
Biometric technologies are reliable	.393	.773	.147	-.156
The cost of maintenance is lower with biometric technologies than with traditional IT security methods	.463	.741	.014	.242
My organization needs to improve the security of its IT assets	.321	-.302	.818	-.063
I am/would be concerned with the technology used by the biometric system	.282	-.189	-.026	.872

Table 24 presents the rotated component structure matrix that shows all loadings on the initial four factors. The component structure matrix loadings present the simple zero-order correlations of each survey item with its corresponding components. The component structure matrix can be useful in interpreting and naming the components (Pett, Lackey, & Sullivan, 2003).



Table 24  
*Rotated Component Structure Matrix*

Item	Component			
	1	2	3	4
I would recommend biometric technologies in my organization	.937	-.143	.012	.031
Biometric technologies are more reliable than traditional IT security methods	.930	.083	-.141	-.034
Biometric technologies provide a significant benefit to my organization	.898	-.126	-.064	.097
I feel that biometrics are secure	.889	-.209	.104	-.046
Biometric hardware is reliable	.868	.144	-.225	.129
I feel that biometric systems use proven technology	.862	.048	-.145	.203
Biometric technologies are more secure than traditional IT security methods	.851	-.238	.123	-.048
I am willing to use biometric technologies to protect sensitive information at my organization	.798	-.111	.208	-.235
Biometric technologies provide a good value for their cost	.753	.383	.353	-.052
My organization needs biometric technologies to secure its IT assets	.682	-.304	-.423	-.225
Biometric technologies were not secure three years ago	-.482	.333	.282	.396
Biometric technologies have considerable cost savings over traditional IT security methods	.128	.828	-.144	-.173
Biometric technologies are reliable	.395	.772	.153	-.144
The cost of maintenance is lower with biometric technologies than with traditional IT security methods	.460	.745	.028	.249
My organization needs to improve the security of its IT assets	.319	-.292	.811	-.055
I am/would be concerned with the technology used by the biometric system	.270	-.175	-.011	.864

There is a fair amount of controversy regarding which matrix, component *pattern* or component *structure* should be the focus of analysis. For example, Harmon (1976), Kline (1994), Nunnally and Bernstein (1994), and Pett, Lackey, and Sullivan (2003) argue that the component structure matrix should be the focus of component identification and interpretation. On the other hand, Tabachnick and Fidell (2001) and Hair, Anderson, Tatham, and Black (1994) argue that the component pattern matrix should be the focus of component interpretation, particularly when the components are highly correlated. Fortunately for this analysis, there were no significant differences between the component structure matrix and the component pattern matrix. Because the correlations among the components were rather low, therefore eliminating one of Hair, Anderson, Tatham, and Black's (1994) main arguments for using the component pattern matrix, and for ease of reading, the remainder of the component identification and interpretation focuses on the component *structure* matrix.

Following recommendations by Comrey and Lee (1992), Guadagnoli and Velicer (1988), and Stevens (2002) that components with less than four loadings above .60 in absolute value are unstable and should not be considered, components two through four were eliminated because of their lack of stability.

As interesting side notes, Item 6 ("My organization needs to improve the security of its IT assets") was the only item with a strong loading (.818/.811) on Component 3 (all other items loaded poorly ( $\leq .423$ )). Likewise, Item 2 ("I am/would be concerned with the technology used by the biometric system") was the only item with a strong loading (.872/.864) on Component 4 (all other items loaded poorly ( $\leq .396$ )). Additionally, Item 9 ("Biometric technologies are reliable"), Item 13 ("The cost of maintenance is lower with

biometric technologies than with traditional IT security methods”), and Item 14 (“Biometric technologies have considerable cost savings over traditional IT security methods”) all loaded reasonably well ( $\geq .741$ ) on Component 2. These findings have implications for the future use of the survey instrument and are discussed in Chapter 5.

Table 25 presents the remaining component and its loadings. Component 1 accounts for 50.135% of the total variance explained.

Table 25  
*Final Component Loadings*

Survey Item	Component 1
I would recommend biometric technologies in my organization	.936
Biometric technologies are more reliable than traditional IT security methods	.929
Biometric technologies provide a significant benefit to my organization	.898
I feel that biometrics are secure	.887
Biometric hardware is reliable	.869
I feel that biometric systems use proven technology	.864
Biometric technologies are more secure than traditional IT security methods	.849
I am willing to use biometric technologies to protect sensitive information at my organization	.795
Biometric technologies provide a good value for their cost	.758
My organization needs biometric technologies to secure its IT assets	.674
Biometric technologies were not secure three years ago	-.470
Biometric technologies have considerable cost savings over traditional IT security methods	.470
Biometric technologies are reliable	.402
The cost of maintenance is lower with biometric technologies than with traditional IT security methods	.320
My organization needs to improve the security of its IT assets	.278
I am/would be concerned with the technology used by the biometric system	.133

## Hypothesis Testing

For the purposes of this study, the four highest correlated survey items identified with each of the four hypotheses were subjected to analysis. Table 26 presents the specific survey items subjected to analysis.

Table 26  
*Hypothesis Testing: Correlation Analysis*

Survey Item	Hypothesis	Correlation Coefficient
I feel that biometrics are secure	Hypothesis 1: An IT/IA manager's decision to recommend biometric security technologies is independent of his/her perception of its security effectiveness	.887
Biometric technologies would/do provide a significant benefit to my organization	Hypothesis 2: An IT/IA manager's decision to recommend biometric security technologies is independent of his/her perceived need for new security technologies	.898
Biometric technologies are more reliable than traditional IT security methods	Hypothesis 3: An IT/IA manager's decision to recommend biometric security technologies is independent of his/her perception of its reliability	.929
Biometric technologies provide a good value for their cost	Hypothesis 4: An IT/IA manager's decision to recommend biometric security technologies is independent of his/her perception of its cost-effectiveness	.758

*Hypothesis 1*

Hypothesis 1 stated (null), an IT/IA manager's decision to recommend biometric security technologies is independent of his/her perception of its security effectiveness. This

hypothesis was evaluated by comparing responses to Item 1 and Item 15 in the survey. Item 1 was, “I feel that biometrics are secure”; Item 15 was, “I would feel comfortable recommending biometric technologies in my organization.” Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*.

Table 27  
*Crosstabulation for Hypothesis 1*

	Biometrics are secure		Totals
	Strongly Agree	Less than Strongly Agree	
I would recommend biometric technologies in my organization			
Strongly Agree	31	2	33
Less than Strongly Agree	8	191	199
Total	39	193	232

Table 28  
*Chi Square Tests for Hypothesis 1*

	Value	Df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	163.659(2)	1	.001		
Continuity Correction(1)	157.292	1	.001		
Likelihood Ratio	127.944	1	.001		
Fisher's Exact Test				.001	.001
Linear-by-Linear Association	162.953	1	.001		
N of Valid Cases	232				

(1) Computed only for a 2x2 table

(2) 0 cells (0.0%) have an expected count less than five. The minimum expected count is 5.55.

Because the  $p$ -value is .001, which is less than 0.05, the null hypothesis was rejected. Therefore, it can be concluded that an IT/IA manager's decision to recommend biometric security technologies is dependent on his/her perception of its security effectiveness.

### *Hypothesis 2*

Hypothesis 2 stated (null), an IT/IA manager's decision to recommend biometric security technologies is independent of his/her perceived need for new security technologies. This hypothesis was evaluated by comparing responses to Item 8 and Item 15 in the survey. Item 8 was, "Biometric technologies would/do provide a significant benefit to my organization"; Item 15 was, "I would feel comfortable recommending biometric technologies in my organization." Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*.

Table 29  
*Crosstabulation for Hypothesis 2*

I would recommend biometric technologies in my organization	Biometric technologies provide a significant benefit		Totals
	Strongly Agree	Less than Strongly Agree	
Strongly Agree	28	5	33
Less than Strongly Agree	1	198	199
Total	29	203	232

Table 30  
*Chi Square Tests for Hypothesis 2*

	Value	Df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	184.115(2)	1	.001		
Continuity Correction(1)	176.484	1	.001		
Likelihood Ratio	134.168	1	.001		
Fisher's Exact Test				.001	.001
Linear-by-Linear Association	183.322	1	.001		
N of Valid Cases	232				

(1) Computed only for a 2x2 table

(2) One cell (25.0%) has an expected count less than 5. The minimum expected count is 4.13.

Because the  $p$ -value is .001, which is less than 0.05, the null hypothesis was rejected. The results, therefore, concluded that an IT/IA manager's decision to recommend biometric security technologies is dependent on his/her perceived need for new security technologies.

### *Hypothesis 3*

Hypothesis 3 stated (null), an IT/IA manager's decision to recommend biometric security technologies is independent of his/her perception of its reliability. This hypothesis was evaluated by comparing responses to Item 10 with Item 15 in the survey. Item 10 was, "Biometric technologies are more reliable than traditional IT security methods"; Item 15 was, "I would feel comfortable recommending biometric technologies in my organization."

Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*.

Table 31  
*Crosstabulation for Hypothesis 3*

I would recommend biometric technologies in my organization	Biometric technologies are more reliable		Totals
	Strongly Agree	Less than Strongly Agree	
Strongly Agree	29	4	33
Less than Strongly Agree	3	196	199
Total	32	200	232

Table 32  
*Chi Square Tests for Hypothesis 3*

	Value	Df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	177.588(2)	1	.001		
Continuity Correction(1)	170.398	1	.001		
Likelihood Ratio	130.653	1	.001		
Fisher's Exact Test				.001	.001
Linear-by-Linear Association	176.822	1	.001		
N of Valid Cases	232				

(1) Computed only for a 2x2 table

(2) One cell (25.0%) has an expected count less than 5. The minimum expected count is 4.55

Because the  $p$ -value is .001, which is less than 0.05, the null hypothesis was rejected. As a result, it can be concluded that an IT/IA manager's decision to recommend biometric security technologies is dependent on his/her perception of its reliability.



*Hypothesis 4*

Hypothesis 4 stated (null), an IT/IA manager's decision to recommend biometric security technologies is independent of his/her perception of its cost-effectiveness. This hypothesis was evaluated by comparing responses to Item 12 and Item 15 in the survey. Item 12 was, "Biometric technologies provide a good value for their cost"; Item 15 was, "I would feel comfortable recommending biometric technologies in my organization." Because a *strongly agree* is the only response that equates to a fully committed recommendation, the responses were coded into two possible categories: *strongly agree* and *less than strongly agree*.

Table 33  
*Crosstabulation for Hypothesis 4*

	Biometric technologies provide a good value for their cost		Totals
	Strongly Agree	Less than Strongly Agree	
I would recommend biometric technologies in my organization			
Strongly Agree	19	14	33
Less than Strongly Agree	0	199	199
Total	19	213	232

Table 34  
*Chi Square Tests for Hypothesis 4*

	Value	Df	Asymp. Sig (2-sided)	Exact Sig (2-sided)	Exact Sig (1-sided)
Pearson Chi-Square	124.796(2)	1	.001		
Continuity Correction(1)	117.256	1	.001		
Likelihood Ratio	86.500	1	.001		
Fisher's Exact Test				.001	.001
Linear-by-Linear Association	124.258	1	.001		
N of Valid Cases	232				

(1) Computed only for a 2x2 table

(2) One cell (25.0%) has an expected count less than five. The minimum expected count is 2.70.

Because the p-value is .001, which is less than 0.05, the null hypothesis was rejected. As a result, it can be concluded that an IT/IA manager's decision to recommend biometric security technologies is dependent on his/her perception of its cost-effectiveness.

#### Summary of Data Collection and Analysis

The overall goal of this research effort was to provide organizational decision makers with improved insight and knowledge into making often difficult and complex security technology adoption decisions. This study examined four facets of an IT/IA manager's willingness to recommend biometric security technologies. It measured the managers' perceptions of the security effectiveness, organizational need, reliability, and cost-effectiveness of biometrics and tested the following four hypotheses:

Hypothesis 1 (null): An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its security effectiveness.

Hypothesis 2 (null): An IT/IA manager's decision to recommend biometric security technology is independent of his/her perceived need for new security technologies.

Hypothesis 3 (null): An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its reliability.

Hypothesis 4 (null): An IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its cost-effectiveness.

None of the null hypotheses were supported by the data collected ( $n = 232, p = .001$ ).

Consequently, the data indicates that an IT/IA manager's decision to recommend biometric security technologies is dependent on his/her perception of its security effectiveness, the need for new security technologies, the new technology's reliability, and its cost-effectiveness.

Chapter 5 presents the results and conclusions of this study, and recommendations for further study.

## CHAPTER 5. STUDY RESULTS, CONCLUSIONS, AND RECOMMENDATIONS

This chapter explores the results and conclusions of the study and provides recommendations for further study on biometric security technologies and related topics. The purpose of the study is to help information technology and information assurance (IT/IA) decision makers select appropriate security solutions for their organizations by focusing on the critical factors contributing to the decision to recommend specific security technologies, in particular the factors that influenced IT/IA managers to recommend biometric security technologies. Specifically, the research can help information technology management professionals determine if the security effectiveness, organizational need, reliability, and cost/value aspects of biometric security technologies are generally acceptable to IT/IA decision makers. The study can also provide security technology companies with information that will assist in the determination of what is important to their customer base when considering the introduction of new IT security products.

Organizational decision making can be quite complicated when considering the adoption of a new technology. Biometric security technology has capabilities, features, and challenges that can make the decision to recommend the technology even more difficult. The overall goal of this research was to give organizational decision makers improved insight and knowledge into making often difficult and complex security technology adoption decisions.

Recent research has indicated that the perceptions of IT/IA managers and professionals are predominant factors in organizational decision making regarding the adoption of security technology (Dynes, Brechbuhl, & Johnson, 2005). Based on Dynes, Brechbuhl, and Johnson's findings, it was appropriate to evaluate the perceptions of IT/IA

managers regarding biometric security technologies and their willingness to recommend or not to recommend biometrics as integral elements in the overall organizational technology adoption decision process. With regard to the evaluation of specific perceptions of technologies, a number of researchers have ascribed the rationale for the choice to recommend a new technology to perceptions of its cost-effectiveness, reliability, organizational need, and function-effectiveness (Craig & Hamidi-Noori, 1985; Ettl, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004).

Drawn from the extant literature and with further development of the relevant concepts, this study investigated four research questions. The research questions studied focused on the association between perceptions of biometric security technologies and managers' decisions to recommend their use. Specifically, the topics of perceived security effectiveness, organizational need, reliability, and cost-effectiveness were measured as independent variables in the decision to recommend biometrics. These perceptions can provide real-life clues into the usefulness of biometric technology and can prove to be a significant factor in the decision to recommend that technology. The specific research questions investigated in this study were as follows:

Question 1: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its security effectiveness?

Question 2: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perceived need for new security technologies?

Question 3: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its reliability?

Question 4: Is an IT/IA manager's decision to recommend biometric security technology independent of his/her perception of its cost-effectiveness?

The study focused on the factors contributing to a manager's decision to recommend or not to recommend a specific security technology. The research results can help decision makers determine what aspects of biometric security technologies are of concern to other professionals, and they may provide vendors with data to help them determine what is important to their customer base. Most importantly, it will help decision makers develop the right solutions for their organizations.

Findings from this research suggest that there are many different factors influencing an IT/IA manager's decision to recommend or not to recommend biometric security technologies. This study indicated that perceptions of biometric security technology, its security effectiveness, the need for the technology, its reliability, and its cost-effectiveness are important considerations in a decision to recommend or adopt the technology in an organization. Across the board, organizations are doing what they can to control expenditures and maximize their returns; this emphasis on cost-effectiveness has become increasingly evident in information technology security where cost-benefit analyses have become a part of a manager's everyday terminology. In the past, organizations often adopted a new security technology in response to perceived new security threats (e.g., scare tactics) only to discover *after implementation* whether it was of value or not. Those days are gone, and IT Security managers are required to perform the same pre-acquisition analyses other business sectors have done for years. For that reason, the study of the influence of critical factors for decision making in the adoption of security technology has become increasingly important.

Often in the security technology field, the benefits and costs of solutions can be difficult to define using strictly financial criteria because of the challenge of quantifying the cost-effectiveness of an upgrade or enhancement to an information security system. Additionally, the intangible benefits and the specific perceptions of technologies in organizations may hold equal or greater weight than purely financial considerations. Consequently, intangible considerations, such as perceived need, security effectiveness, and reliability when evaluated in tandem with financial considerations, such as cost-effectiveness, may result in better decisions by managers. This study focused on the intangibles that help determine whether an IT/IA professional will choose to recommend/adopt biometric security technologies.

## Hypotheses

### *Hypothesis 1*

Hypothesis 1 stated (null), an IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its security effectiveness. The Chi Square Test of Independence resulted in the researcher rejecting the null hypothesis ( $p = .001$ ) and concluding that the decision to recommend biometrics is dependent on a manager's perception of its security effectiveness.

### *Hypothesis 2*

Hypothesis 2 stated (null), an IT/IA manager's decision to recommend biometric security technology is independent of his/her perceived need for new security technologies. The Chi Square Test of Independence resulted in the researcher rejecting the null hypothesis

( $p = .001$ ) and concluding that the decision to recommend biometrics is dependent on a manager's perceived need for new security technologies.

### *Hypothesis 3*

Hypothesis 3 stated (null), an IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its reliability. The Chi Square Test of Independence resulted in the researcher rejecting the null hypothesis ( $p = .001$ ) and concluding that the decision to recommend biometrics is dependent on a manager's perception of its reliability.

### *Hypothesis 4*

Hypothesis 4 stated (null), an IT/IA manager's decision to recommend biometric security technology is independent of his/her perception of its cost-effectiveness. The Chi Square Test of Independence resulted in the researcher rejecting the null hypothesis ( $p = .001$ ) and concluding that the decision to recommend biometrics is dependent on a manager's perception of its cost-effectiveness.

### *Hypothesis Testing Summary*

This research effort examined four facets of an IT/IA manager's willingness to recommend biometric security technologies. All of the factors (security effectiveness, need, reliability, and cost-effectiveness) contributed to a manager's willingness to recommend the use of biometric security technologies in their organizations. None of the null hypotheses were supported by the data collected ( $n = 232, p = .001$ ). Consequently, the data indicates that an IT/IA manager's decision to recommend biometric security technologies is dependent



on his/her perception of its security effectiveness, the need for new security technologies, its reliability, and its cost-effectiveness.

### Study Design

The theoretical study population consisted of all IT/IA professionals in a management role. The study population was 232 IT/IA professionals affiliated with the Northern Virginia Chapter of the Information Systems Security Association (ISSA-NOVA) who volunteered to participate in the study. It was assumed that IT/IA professionals who are affiliated with ISSA-NOVA and who volunteered to complete online surveys are without significant differences in their attitudes than all other IT/IA professionals in the Mid-Atlantic (Maryland, Virginia, and the District of Columbia) area. The sampling frame contained 382 IT/IA professionals on ISSA-NOVA's email directory and represented small, medium, and large-sized organizations. The study did not require that a manager support a particular number of users, only that he/she was familiar with biometric security technologies.

Randomness of the target sample was preserved because each member of the sample had an equal opportunity to complete the survey. Each of the 382 IT/IA professionals on ISSA-NOVA's mailing list were emailed a survey invitation with a link to the survey Web site in the text. Additionally, ISSA-NOVA publicized the study by allowing the researcher to announce the study at regularly scheduled monthly meetings, and to provide a link to the survey Web site through the ISSA-NOVA Web site ([www.issa-nova.org](http://www.issa-nova.org)), and to publish announcements in the ISSA-NOVA Newsletter.

The survey was hosted by Survey Monkey ([www.surveymonkey.com](http://www.surveymonkey.com)), a professional Web survey hosting company, and was available to participants via the Internet. Participants were anonymous when completing the survey. A limit of "one response per respondent" was controlled to prevent multiple responses. After completing the survey, participants were prevented from entering additional responses. However, participants who did not complete the survey in one visit, could return one or more times to complete the survey and be taken to the point that they had left off. The survey responses were downloaded by the researcher and exported into Statistical Package for the Social Sciences (SPSS) 13 for analysis. Outlier detection was conducted and data entry errors were corrected. Reliability was re-validated through the use of Cronbach's alpha, with a resulting alpha of 0.89.

The first section of the survey was designed to evaluate managers' perceptions of biometric security technologies as they relate to security effectiveness. The second section assessed the respondents' perception of biometric security technologies as they relate to the need for biometrics in their organization. The third section evaluated managers' perceptions of the reliability of biometric security technologies. The fourth section provided a perspective of the respondents' attitudes toward the cost-effectiveness of biometric security technologies. The fifth section provided an understanding of the managers' willingness to recommend biometric security technologies to their organizations. A five-point Likert scale (*strongly disagree* = 1 to *strongly agree* = 5) was used for sections one through five. The last section of the survey instrument identified demographics for future research purposes, such as experience with biometrics, number of users, title/job function, and industry.

### Discussion of the Findings

The results of the Chi Square Tests of Independence supported four of the four hypotheses and indicated that a manager's decision to recommend biometric security technology in his/her organization is dependent on his/her perception of its security effectiveness, the organizational need for biometrics, its reliability, and its cost-effectiveness. The results also made intuitive sense, because security-effectiveness, organizational need, reliability, and cost-effectiveness have become increasingly important topics in IT security literature.

These findings help to understand the factors surrounding the willingness of managers to recommend biometric security technologies. It shows that there are multiple aspects involved in a manager's decision to recommend or not to recommend a biometric security solution in their organization – and vendors and managers should be aware that technology adoption often requires many perceived benefits to be present. These multiple decision factors indicate that organizations must recognize a need for the technology, and that the technology be considered secure, reliable, and cost-effective before solutions affecting their existing security architecture will be recommended. These four decision factors provide a key perspective into the future of technology adoption, infusion, and decision making for IT executives.

Additional research may be done to assess the influence of previous experiences with biometric security technologies and a manager's willingness to recommend biometrics. As shown in this study, there appears to be a positive and increasing correlation between years of experience with biometrics and the respondents' willingness to recommend biometrics.

This indication of greater acceptance of biometric security technology as one's experience with it increases may merely be a reflection of the growing maturity of biometrics or it may be a clue to the target audience of decision makers.

Further study of the impact that the size of the organization may have on an individual's willingness to recommend biometric security technologies may also yield important implications. In this study, it appeared that mid-size to large organizations (fifty users to less than 5,000 users) may be more willing to adopt biometric security technologies than organizations supporting either very small or very large numbers of users. This willingness to recommend biometrics may be caused by mid-size to large organizations being large enough to have the in-house technical expertise and financial resources to implement biometrics (compared to smaller organizations) and/or a sufficiently large user base to make biometrics cost-effective (again, compared to smaller organizations).

Title/job function and industry do not appear to have measurable influences on a manager's comfort, authority, and desire to recommend or not to recommend biometrics based on the four criteria in the study. The study indicates that many factors play a role in the decision to recommend and/or adopt a technology. Further study could indicate which factor or confluence of factors exerts the greatest influence on the adoption of technology. Nevertheless, it can be concluded that IT/IA managers evaluate technology based on multiple criteria, and that before funding a project, executives should require substantial research and information related to the security-effectiveness, organizational need, reliability, and cost-effectiveness of technology critical to the organization.

### Implications of the Study

#### *For the Researcher*

Researchers have often attributed the slow (relative to other security technologies) adoption of biometric security technologies to the technical complexities concomitant with the technology, often ignoring or giving little attention to non-technical considerations that might influence the decision making process and/or impact implementation. This study provides evidence that several non-technical factors influence a manager's decision to recommend/adopt biometric security technologies. From a research perspective, these non-technical decision factors can not be ignored. Future researchers need either to evaluate the influence of these factors directly or to consider their potential as shadow variables.

#### *For the Practitioner*

The recommendations proposed for the practitioner are based on the findings and conclusions of this study. The empirical evidence arrived at in this study attempted to identify the critical factors that explain why managers choose to recommend new technologies to their organizations. It is recommended that organizations considering adopting new security technologies should give serious attention to the perceived effectiveness, need, reliability, and cost-effectiveness of the new technology.

Another implication of this study for the practitioner is the strong indication that there are non-technical factors affecting an IT/IA manager's decision to recommend/adopt biometric security technologies. The identification of these factors is important because the prevalent literature dealing with selection and implementation of biometrics focuses almost exclusively on the technical considerations relevant to selecting a particular biometric

solution. When non-technical issues are addressed, they are usually limited to users' fears about ethical considerations and the perceived invasiveness of the technology, without considering the attitudes and perceptions of IT/IA managers who may need to champion the technology.

In selecting a biometric authentication system and preparing for its implementation, organizations should expand their focus from the issues of technology to include the influence of the non-technical decision factors identified in this study. It is important that organizations consider not only the technical impediments to effective implementation but also the potential psychological impediments such as managers' attitudes and perceptions about biometrics and user fears about the technology.

This study presents implications for biometric and traditional security vendors too. Historically, biometric security vendors have concentrated on differentiating their products by establishing technical specifications superior to their competitors. This study presents evidence that superior technical specifications are not the sole rationale for a manager's decision to recommend or not to recommend biometric security technologies. Based on the research in this study, security vendors should expand their marketing focus to address the non-technical decision factors of perceived security effectiveness, organizational need, reliability, and cost-effectiveness.

### Suggestions for Further Research

Several fascinating topics can expand the research underlying this study. The study could be replicated using a nationwide or international sample of IT/IA professionals. One

advantage of this expanded study would be the potential for results that are more readily generalizable to the population of IT/IA professionals. Examples of this type of expanded sample are the membership of the International Systems Security Association (ISSA – the parent organization of the chapter sampled for this study) and the membership of the International Information Systems Security Certification Consortium.

Another related study effort might be to conduct a similar survey that changes the research approach of the study. Rather than an Internet-mediated survey, conducting live surveys with IT/IA professionals attending an IT security conference might prove insightful. While the results may be similar overall, the open-ended responses that come from interviews may add valuable insights and perspectives to the findings. An additional research alternative might be to use the existing sample data (comprised of data collected from members of ISSA-NOVA, a regional association of IT/IA professionals) and compare the similarities and dissimilarities of the responses to a sample that is more readily generalizable to the population of IT/IA professionals (i.e., the membership of the ISSA) within the U.S. or internationally. Further research may also be done on the existing data set to evaluate the influence organization size and prior use of the technology has on decision making. The research may be revised to fit other technologies or solutions as a whole or may be revisited to understand the most significant predictor of the willingness of management to recommend a technology-based solution.

An additional research effort could focus on the relative influences of technical issues versus attitudes and perceptions in the decision making process when considering biometric security technologies. Such a study might reveal surprising correlations between perceptions

of a specific biometric technology versus other biometric technologies. The study could also be very useful to companies marketing and/or developing biometric solutions because it would provide additional insight into the marketing and sales cycle for biometrics.

As indicated in the study, there appeared to be a positive and increasing correlation between years of experience with biometric security technologies and IT/IA managers' willingness to recommend biometrics. It would be interesting to determine whether this indication of greater acceptance of biometric security technology as one's experience with it increases is unique to IT security technologies or if it is generally indicative of other IT technologies or other technologies in general.

The research also indicated that IT/IA managers in mid-size to large organizations (50 users to less than 5,000 users) may be more willing to recommend biometric security technologies than managers supporting very large (5,000 or more) numbers of users. Intuitively, it would seem that larger organizations would be more likely to have the in-house expertise, financial resources, and project management capability than smaller-sized organizations. Additional research into this area could provide information useful to understanding why it appears that managers supporting very large numbers of users appear to be less likely to embrace biometrics than managers in smaller organizations are.

Security is an important topic with continually increasing threats to organizational information assets and newly exposed vulnerabilities in security products. A researcher may choose to explore the evolution of individual security products, such as the shift from "intrusion detection" systems to "intrusion prevention" systems. Another research area for individual components of security could be authentication and authorization methods and



changes to their effectiveness when supplemented with other security methods, such as encryption and biometrics.

In addition, within the security domain, research into security compromises of various technologies could yield significant findings. For example, the study of security breaches in biometric security technologies as they relate to banking and healthcare (both environments where privacy is critical) may provide insight into what works, what does not work, what organizations can count on, and what provides the best cost-benefit for organizations.

Another related topic of study is the question of why some organizations adopt a particular new security technology while other organizations in the same industry outright reject the same technology. Researchers have not reached any generalizable theory that can predict the adoption or rejection of new IT (or IT security) technologies in organizations.

Future researchers may choose to study the true reliability of hardware and software as a single working component in order to ascertain what organizations can really rely on as opposed to manufacturers' mean-time-between-failure (MTBF) statistics. Researchers may explore whether MTBF is an accurate measure of what organizations experience in hardware and software failure and might explore what combination of the two is most reliable.

Research into hardware and software reliability suggests a study in partner testing (for example, software developers testing their software on a particular hardware platform) and may uncover results useful to the evaluation of specific hardware and software configurations.

Finally, there are several topics related to the cost-effectiveness of IT security that an economic-minded researcher may wish to explore. Do organizations post-test their

cost-benefit assumptions and do a gap analysis? How are variances tolerated in IT security? How important are the C-level executives' opinions of security technology, or do IT professionals ultimately have the final say in most organizations? Research may also be conducted to find out how smaller companies compare in their IT spending to independent variables, such as the number of users or their profitability.

#### *Survey Instrument Considerations*

As previously discussed in Chapter 4, the factor analysis indicated that Item 6 (“My organization needs to improve the security of its IT assets”) was the only item with a strong loading (.818/.811) on Component 3 (all other items loaded poorly ( $\leq$  |.423|)). Likewise, Item 2 (“I am/would be concerned with the technology used by the biometric system”) was the only item with a strong loading (.872/.864) on Component 4 (all other items loaded poorly ( $\leq$  |.396|)). Further, in the test-retest sequence, Item 2 was one of the two survey items with observed differences between Test 1 and Test 2, indicating the possibility of item instability.

Additionally, Item 9 (“Biometric technologies are reliable”), Item 13 (“The cost of maintenance is lower with biometric technologies than with traditional IT security methods”), and Item 14 (“Biometric technologies have considerable cost savings over traditional IT security methods”) all loaded reasonably well ( $\geq$  |.741|) on Component 2, while all other items loaded poorly ( $\leq$  |.383|).

Future researchers who wish to use the survey instrument may wish to consider testing the questionnaire without Items 2, 6, 9, 13, and 14 because these items appear to measure, to a large extent, different aspects of managers' perceptions of biometric security technologies. Additionally, the apparent lack of stability for Item 2 is further cause for

segregating the Item from the survey instrument. On the other hand, it may prove interesting to refine further the specific elements that these five survey items measure by testing the use of the five items in different environments and/or with different populations.

### Conclusions

The principal objective of this study was to investigate the critical factors that influence IT/IA managers to recommend or not to recommend biometric security technologies. The research conducted under this study offers an understanding of the reasons that IT/IA managers choose to recommend or not to recommend particular technologies, specifically biometric security, to their organizations. IT/IA managers' perceptions were the focus of the study because research has shown that IT/IA managers' recommendations were the primary drivers of organizational adoption of IT security products and technologies like biometrics (Dynes, Brechbuhl, & Johnson, 2005). Further, as discussed in Chapter 2, numerous researchers have ascribed the rationale for the choice to recommend a new technology to perceptions of its cost-effectiveness, reliability, organizational need, and function-effectiveness (Craig & Hamidi-Noori, 1985; Ettl, 2000, 1986; Gerwin, 1982; Gunn, 1982; Meridith & Hill, 1987; Putnam, 1987; Roberts & Pick, 2004). These four areas provided the foundation to develop a set of factors and research questions for this empirical research effort. The research questions then became the basis of the study's stated hypotheses examining managers' perceptions of the security effectiveness, need, reliability, and cost-effectiveness of biometrics. Each of these perceptual areas was correlated with the managers' decision to recommend or not to recommend biometric security technologies. Data was

collected through a survey administered to 232 members of the International Systems Security Association (ISSA), a professional association of IT/IA managers and professionals. The data was evaluated and statistical analyses were conducted to test the stated hypotheses for this study and to provide the descriptive results.

Based on the analyses of data and testing of the stated hypotheses for this study, the findings indicate that a new security technology with higher levels of perceived security-effectiveness, organizational need, reliability, and cost-effectiveness will have a greater prospect for being recommended for adoption by IT/IA managers. These findings significantly contribute to the data in the fields of information technology and information assurance (security). They added new knowledge in these fields and highlighted the importance of the perceptions of IT/IA managers regarding biometric security technologies. The research showed that security effectiveness, need, reliability, and cost-effectiveness are reasons why technology managers choose to recommend biometric security technologies. These findings can help determine business reasons for IT/IA managers' recommendations to adopt biometric technology.

The study also presented insight into why IT/IA professionals may recommend one biometric security technology over another and offered some areas for consideration to organizations contemplating the use of biometric security technology. Additionally, the study provided security technology companies and developers of information security products with information to assist in the determination of what is important to their customer base when considering the introduction of new IT security products. In the future, business and

technology managers will be interested in this data when contemplating the adoption of biometric security technologies.

## REFERENCES

- Abelson, R.P. (1976). Script processing in attitude formation and decision making. In J.S. Carroll & J.W. Payne (Eds.), *Cognition and Social Behavior*, Hillsdale, NY: Lawrence Erlbaum.
- Agarwal, R. & Prasad, J. (2000, August). A field study of the adoption of software process innovations by information systems professionals. *IEEE Transactions on Engineering Management*, 47(3), 295-308.
- Agarwal, R. (1998, January). The antecedents and consequents of user perceptions in information technology adoption. *Decision Support Systems*, 22(1), 15-29.
- Ajzen, I. (1988). *Attitudes, personality, and behavior*. Chicago: The Dorsey Press.
- Ajzen, I. & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.
- Alliance for Telecommunications Industry Solutions (ATIS). (2005). Retrieved June 4, 2005 from [http://www.atis.org/tg2k/\\_information\\_assurance.html](http://www.atis.org/tg2k/_information_assurance.html).
- Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. *Ethics and Information Technology*, 5(3), 139-150.
- Ammenheuser, M. (2002, February). The business case for biometrics. *Bank Systems & Technology*, 39(2), 42.
- Anderson, R.J. (2001). *Security engineering: A guide to building dependable distributed systems*. New York: John Wiley & Sons.
- Ashbourn, J. (2004). *Practical biometrics: From aspiration to implementation*. London: Springer-Verlag.
- Au, Y.A. & Kauffman, R.J. (2003). Information technology investment and adoption: A rational expectations perspective. *Proceedings of the 36<sup>th</sup> Hawaii International Conference on System Sciences*, IEEE Computer Society, 1-10.
- "Authentication questions and answers." (2002, March 18). *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargt.com>.
- Babbie, E. (2003). *The practice of social research*. Belmont, CA: Wadsworth.
- "Banking on biometrics." (2004, April). *Security*, 41(4), 39.

- Barcikowski, R.S. & Stevens, J.P. (1975). A Monte Carlo study of the stability of canonical correlations, canonical weights, and canonical variate-variable correlations. *Multivariate Behavioral Research*, 10, 353-364.
- Baron, R. & Kenny, D. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 31(6), 1173-1182.
- Bergstrom, R.P. (1987, July). Critical issues in CIM implementation. *CIM Technology*, 5-6.
- Beyer, J.M. & Trice, H.M. (1978). *Implementing Change: Alcoholism Policies in Work Organizations*. New York: Free Press.
- “Beyond doors: Securing records with finger flick.” (2002). *Security*, 39(7), 57.
- Bing, H.E., Zheng-ding, Q., & Dong-mei, S. (2002). A secure mechanism for network authentication combining hand shapes verification and encryption. *ICSP'02 Proceedings*, 1846-1850.
- “Biometrics are opening many eyes.” (2004, February). *Bank Technology News*, 17(2), 54.
- “Biometrics identification.” (2003, February 17). *Journal of Commerce*, 1.
- “Biometrics not yet ready to secure corporate IT.” (2004, September 21). *Computer Weekly*, 1.
- “Biometrics, trusted computing key to securing laptops, handhelds.” (2004, January 17). *Eweek*, 1.
- Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., & Senior, A.W. (2004). *Guide to biometrics*. New York: Springer-Verlag.
- Boroshok, J. (2005a, January 14). Pointing the finger at biometrics. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargt.com>.
- Boroshok, J. (2005b, January 15). Will 2005 measure up as the year of business biometrics? *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargt.com>.
- Brancheau, J.C. & Wetherbe, J.C. (1990, June). The adoption of spreadsheet software: Testing innovation diffusion theory in the context of end-user computing. *Information Systems Research*, 1(2), 115-143.

- “Bringing biometrics to e-commerce: James Uberti speaks out on new solutions.” (2003, July 21). *Electronic Commerce News*, 1.
- Callas, J. (2003, June 20). Considerations for biometric use. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtarg.com>.
- Carmines, E.G. & Zeller, R.A. (1979). *Reliability and validity assessment*. Thousand Oaks, CA: Sage.
- Center for Digital Strategies (2005). Information security field study. Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business, Dartmouth University. Retrieved August 27, 2005 from <http://mba.tuck.dartmouth.edu/digital/Research/ResarchHighlights/Security>.
- Chandra, A. & Calderon, T.G. (2003). Toward a biometric security layer in accounting systems. *Journal of Information Systems*, 17(2), 51-70.
- Chapple, M. (2003, September 30). Practical biometrics. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtarg.com>.
- Chirillo, J. & Blaul, S. (2003). *Implementing biometric security*. Indianapolis, IN: Wiley.
- Cohen, M.D., March, J.G., & Olsen, J.P. (1972, March). A garbage can model of organizational choice. *Administrative Science Quarterly*, 17(1), 1-25.
- Collins, P.D., Hage, J., & Hull, F.M. (1988, September). Organizational and technological predictors of change in automaticity. *Academy of Management Journal*, 31(3), 512-543.
- Comrey, A.L. & Lee, H.B. (1992). *A first course in factor analysis*. Hillsdale, NY: Lawrence Erlbaum.
- Conole, G. & Oliver, M. (1998). A pedagogical framework for embedding C&IT into the curriculum. *Association for Learning Technology Journal*, 6(2), 4-16.
- Cook, T. & Campbell, D. (1979). *Quasi-experimentation: Design and analysis issues*. Boston: Houghton Mifflin.
- Costlow, T. (2003, June 2). Lack of standards slows adoption: Large companies are waiting for interoperability. *Design News*, 58(8), 38-40.
- Craig, R. & Hamidi-Noori, A. (1985). Recognition and use of automation: A comparison of small and large organizations. *Journal of Small Business and Entrepreneurship*, 3(1), 37-44.



- Daft, R.L. & Becker, S.W. (1981). *Innovation in organizations*. New York: Elsevier Press.
- Dasgupta, S., Agarwal, D., Ioannidis, A., & Gopalakrishnan, S. (1999). Determinants of information technology adoption: An extension of existing models to firms in a developing country. *Journal of Global Information Management*, 7(3), 30-65.
- Davis, F.D. (1989, September). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.
- Dawes, R.M. (1979). The robust beauty of improper linear models in decision making. *American Psychologist*, 34, 571-582.
- Downs, Jr., G.W. & Mohr, L.B. (1976, December). Conceptual issues in the study of innovation. *Administrative Science Quarterly*, 21(4), 700-714.
- Dunn, R. (2004). Is your security system accurate? *Security*, 41(4), 46-47.
- Dunstone, E.S. (2001). Emerging biometric developments: Identifying the missing pieces for industry. *International Symposium on Signal Processing and its Applications (ISSPA)* (August 13-16, Kuala Lumpur, Malaysia), 351-354.
- Duxbury, L., Decady, Y., & Tse, A. (2002). Adoption and use of computer technology in Canadian small businesses: A comparative study. In S. Burgess (Ed.), *Managing Information Technology in Small Business: Challenges and Solutions* (19-47). London: Idea Group Publishing/Information Science Publishing.
- Dynes, S., Brechbuhl, H., & Johnson, M.E. (2005). Information security in the extended enterprise: Some initial results from a field study of an industrial firm. Working Paper Series 05-1. *Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth*. Retrieved August 26, 2005 from <http://mba.tuck.dartmouth.edu/digital/Research/AcademicPublications/InfoSecurity.pdf>
- Erdos, P.L. (1983). *Professional mail surveys*. New York: Krieger.
- Ettlie, J.E. (2000). *Managing technological innovation*. New York: John Wiley & Sons.
- Ettlie, J.E. (1986). Implementing manufacturing technologies: Lessons form experience. In D.D. Davis (Ed.), *Managing Technological Innovation*. San Francisco: Jossey-Bass, 72-104.
- Ettlie, J.E. & Vallenga, D.B. (1979, May). The adoption time period for some transportation innovations. *Management Science*, 25(5), 429-443.

- Faundez-Zanuy, M. (2004, June). On the vulnerability of biometric security systems. *IEEE A&E Systems Magazine*, 3-8.
- Feder, B. (2003, February 24). Note: Apply moisturizer only after gaining access. *New York Times*, C5.
- Ferraro, C. (2003, September 22). Cost savings, security through identity management. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargget.com>.
- Fischhoff, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9, 127-152.
- Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Fowler, F.J. (2001). *Survey research methods*, (3rd ed.). Thousand Oaks, CA: Sage.
- Gerwin, D. (1982, March-April). Do's and don'ts of computerized manufacturing. *Harvard Business Review*, 60(2), 107-116.
- Gianus Technologies, Inc. (2003, February 13). *Beyond encryption: Absolute data protection through invisibility*. White Paper. New York: Gianus Technologies, Inc. Retrieved February 4, 2005 from <http://www.gianus.com>.
- Gips, M.A. (2002, August). Face recognition blasted again. *Security Management*, 46(8), 18.
- Glass, B. (2004, January 20). Biometric security: Someday biometric systems may play an important role in security all kinds of systems, but they're not foolproof yet. *PC Magazine*, 23(1), 66.
- "Government catches biometrics bug." (2005). *Security*, 42(1), 18.
- Grimes, B. (2003, April 22). Biometric security: Case study businesses are getting their feet wet with fingerprint, iris and face recognition technology. *PC Magazine*, 22(7), 74.
- Grover, V., Teng, J.T.C., & Fiedler, K.D. (1998). IS investment priorities in contemporary organizations. *Communications of the ACM*, 41(2), 40-48.
- Groves, E. & Aston, A. (2004, April 12). To make a quick I.D., play it by ear. *Business Week*, 92.

- Guadagnoli, E. & Velicer, W.F. (1988). Relation of sample size to the stability of component patterns. *Psychological Bulletin*, 103(2), 265-275.
- Gunn, T.G. (1982, September). The mechanization of design and manufacturing. *Scientific American*, 115-130.
- Gurliacci, D. (2004, May 10). Smaller companies begin to use biometrics, forgetting about passwords. *Fairfield County Business Journal*, 5.
- Hair, J.F., Anderson, R.E., Tatham, R.L., & Black, W.C. (1995). *Multivariate data analysis with readings* (4th ed.). Englewood Cliffs, NJ: Prentice-Hall.
- Hamidi-Noori, A. & Templer, A. (1983). Factors affecting the introduction of robots. *International Journal of Operations and Production Management*, 3(2), 46-57.
- Hamilton, D.P. (2003, September 29). Workplace security; read my lips: Are biometric systems the security solution of the future? *Wall Street Journal*, R4.
- Hammond, K.R., McClelland, G.H., & Mumpower, J. (1980). *Human judgement and decision making*. New York: Praeger.
- Hannah, G. (2005, January). Is it time to change your company's time and attendance system? *IOMA's Payroll Manager's Report*, 5(1), 5-7.
- Harmon, H.H. (1976). *Modern factor analysis* (3rd ed.). Chicago: University of Chicago Press.
- Harris, A.J. & Yen, D.C. (2002). Biometric authentication: Assuring access to information. *Information Management & Computer Security*, 10(1), 12-19.
- Harrison, E.F. (1998). *The managerial decision making process* (5th ed.). Boston: Houghton-Mifflin.
- Henderson, J.C. & Nutt, P.C. (1978, October). Modeling organizational decisions using the human problem solving paradigm. *Academy of Management Review*, 3(4), 762-773.
- Higbie, C. (2004, March 30). Authentication and access. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtarg.com>.
- Hill, J.A. (2001, November). Biometrics come of age. *Internet World*, 7(19), 54.
- Hogan, H. (2004, April 26). Can your fingerprint be compromised? *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtarg.com>.

- Hulme, G.V. (2003, February 10). Slow acceptance for biometrics. *Information Week*, 56-62.
- Hurley, E. (2003, September 30). Biometrics may be too pricey, complex for data center. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargt.com>.
- Hwang, D.D. & Verbauwhede, I. (2004). Design of portable biometric authenticators – energy, performance, and security tradeoffs. *IEEE Transactions on Consumer Electronics*, 50(4), 1222-1231.
- International Biometric Group. (2005). Biometrics Market and Industry Report 2004-2008. Retrieved June 4, 2005 from [http://www.biometricgroup.com/reports/public/market\\_report.html](http://www.biometricgroup.com/reports/public/market_report.html).
- Imparato, N. (2002, April 16). Does face recognition have a future? *Intelligent Enterprise*, 5(7), 20-21.
- Isenberg, D.J. (1984, November/December). How senior managers think. *Harvard Business Review*, 62(6), 81-90.
- Jackson, W. (2002, August 26). NIST identifies good and bad points of biometrics. *Government Computer News*, 21(25), 1.
- Jain, A.K. (2004). Biometric recognition: How do I know who you are. *IEEE Symposia*, 3-5.
- Jonietz, E. (2004, June). Boosting biometrics: Multiple identity measurements are the key to better security. *Technology Review*, 107(5), 20-22.
- Kaine, A.K. (2003). The impact of facial recognition systems on business practices within an operational setting. *25<sup>th</sup> International Conference Information Technology Interfaces*, (June 16-19, Cavtat, Croatia), 315-320.
- Kaiser, H.F. (1974, March). An index of factorial simplicity. *Psychometrika*, 39(1), 32-36.
- Kelley, P. & Kransbrg, M. (Eds.). (1978). *Technological innovation: A critical review of current knowledge*. San Francisco: San Francisco University Press.
- Khazanchi, D. (2005). Information technology (IT) appropriateness: The contingency theory of 'fit' and IT implementation in small and medium enterprises. *Journal of Computer Information Systems*, 45(3), 88-95.
- Kilborn, P.T. (2002, February 20). Your thumb here: Newest ID of choice at store and on job. *New York Times*, A1.

- Kimberley, J.R. (1981). Managerial innovation. In P. Nystrom & W. Starbuck (Eds.), *Handbook of Organizational Design*, New York: Oxford University Press, 84-110.
- Kimberley, J.R. & Evanisco, M.J. (1981). Organizational innovation: The influence of individual, organizational and contextual factors on hospital adoption of technological and administrative innovations. *Academy of Management Journal*, 24(4), 689-713.
- Kish, L. (1995). *Survey sampling*. New York: Wiley-Interscience.
- Kleist, V.F., Riley, R.A., & Pearson, T.A. (2005). Evaluating biometrics as internal control solutions to organizational risk. *Journal of American Academy of Business*, 6(2), 339-343.
- Kline, P. (1994). *An easy guide to factor analysis*. New York: Routledge.
- Koch, C. (2002, September 15). The powers that should be; IT decisions have to reflect the goals of the business and engage the attention of the business. *CIO*, 15(23), 48-54.
- Kolodgy, C.J. (2003, June). Identity management in a virtual world. *IDC White Paper*, n.p.
- Kresbsbach, K. (2003, November). The rise of biometrics: The factor that will push more U.S. financial firms into adopting biometrics is fraud and ID theft. *Bank Technology News*, 16(11), 54-56.
- Kwon, T.H. & Zmud, R.W. (1987). Unifying the fragmented models of information systems implementation. In R.J. Boland & R.A. Hirschheim (Eds.), *Critical Issues in Information Systems Research*, New York: John Wiley & Sons..
- Lai, V.S. & Guynes, J.L. (1997). An assessment of the influence of organizational characteristics on information technology adoption decision: A discriminative approach. *IEEE Transactions on Engineering Management*, 44(2), 146-157.
- Lanzi, S. (2002, June). Determining worthwhile IT security efforts. *Pulp & Paper*, 76(1), 25-26.
- Lavidge, R.J. & Steiner, G.A. (1961, October). A model for predictive measurements of advertising effectiveness. *Journal of Marketing*, 25(6), 59-62.
- Lawlor, M. (2005, February). Debunking information security myths. *Signal*, 59(6), 39-42.
- Leahy, K. (1988). Statistical power and sample size determination. *Direct Marketing*, 50(11), 28-30.

- Ledford, J.L. (2002, June). The Rolls Royce of security: Are biometrics worth the expense? *New Architect*, 7(6), 14-15.
- Lesk, M. (2003). The mindset of dependability. *Communications of the ACM*, 46(1), 136.
- Levine, L. (2004, March). Cost-justifying managed security for financial institutions. *Community Banker*, 13(3), 64-65.
- Lewis, P. (2005, January 24). Let your fingers do the locking. *Fortune*, 151(2), 42-44.
- Liddle, A.J. (2004, September 13). Employee bios: Operators find workers' fingerprint data good reading. *Nation's Restaurant News*, 38(37), 76.
- Likert, R.A. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, No. 140, 4-53.
- Liu, S. & Silverman, M. (2001, January/February). A practical guide to biometric security technology. *IT Pro*, 27-32.
- Madansky, A. (1990). Sample size determination. *Applied Marketing Research*, 30(2), 48-50.
- Maher, K. (2003, November 4). Big employer is watching: Companies monitor workers with high-tech systems: Did lunch take too long? *Wall Street Journal*, B1.
- Mangione, T.W. (1995). *Mail surveys: Improving the quality*. Thousand Oaks, CA: Sage.
- March, J.G. & Olsen, J.P. (1976). *Ambiguity and choice in organizations*. Bergen, Norway: Universitetsforlaget.
- March, J.G. & Shapira, Z. (1999). Behavioral decision theory and organizational decision theory. In Ungson, G.R. & Braunstein, D.N. (Eds.), *Decision Making: An Interdisciplinary Inquiry*, Boston: PWS Publishing, 92-115.
- Margulius, D.L. (2004, July 5). Biometrics move into the mix – future role is likely to be supplemental to smart cards and passwords. *InfoWorld*, 26(27), 19.
- Markowitz, J. (2002, January 31). Biometrics gaining more identity as security option. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargget.com>.
- Matyáš, V. & Riha, Z. (2003, May/June). Toward reliable user authentication through biometrics. *IEEE Security & Privacy*, 45-49.

- McHale, J. (2003, December). Biometrics: The body's keys: The use of biometrics such as face, iris, and fingerprint is becoming one of the most effective ways to provide secure access control, yet the lack of significant government funding is slowing the growth of the technology. *Military & Aerospace Electronics*, 14(12), 17-23.
- Mercuri, R.T. (2003, June). Analyzing security costs. *Communications of the ACM*, 46(6), 15-18.
- Meredith, J.R. & Hill, M.M. (1987, Summer). Justifying new manufacturing systems: A managerial approach. *Sloan Management Review*, 28(4), 49-61.
- Messick, S. (1998). Test validity: A matter of consequence. *Social Indicators Research*, 45(1-3), 35-44.
- Messmer, E. (2002, October 7). Is biometrics ready to bust out? *Network World*, 24.
- Meyer, A.D. & Goes, J.B. (1988). Organizational assimilation of innovations: A multilevel contextual analysis. *Academy of Management Journal*, 31(4), 897-923.
- Mintzberg, H., Raisinghani, D., & Theoret, A. (1976, June). The structure of unstructured decision processes. *Administrative Science Quarterly*, 21(2), 246-275.
- Mitroff, I.I. & Emshoff, J.R. (1979, January). On strategic assumption making: A dialectical approach to policy and planning. *Academy of Management Review*, 4(1), 1-12.
- Moreno-Robello, J. (1999). Estimating the unknown sample size. *Journal of Statistical Planning and Inference*, 83, 311-318.
- Morris, B.R. (2002, January 17). Tracking work hours by touch, not a punch. *New York Times*, G6.
- Morrissey, J. (2002, November 25). Access denied; Mayo Clinic is a believer in using biometrics to protect medical data, but technological flaws shut doctors out, shut systems down. *Modern Healthcare*, 32(47), 22-30.
- Murphy, S. & Bray, H. (2003, September). Face recognition fails at Logan; eye scan rejected. *Boston Globe*, A1.
- Myers, R. (1990). *Classical and modern regression with applications* (2nd ed.). Boston, MA: Duxbury Press.
- Nanavati, S., Thieme, M., & Nanavati, R. (2002). *Biometrics: Identity verification in a networked world*. New York: John Wiley & Sons, Inc.

- Newell, A. & Simon, H.A. (1972). *Human problem solving*. Englewood Cliffs, NJ: Prentice-Hall.
- Nguyen, H.T. (2004, December). Beyond ROI: A new framework for measuring the value of technology investments. *Government Finance Review*, 20(6), 30-36.
- Nixon, M.S., Carter, J.N., Grant, M.G., Gordon, L., & Hayfron-Acquah, J.B. (2003). Automatic recognition by gait: Progress and prospects. *Sensor Review*, 23(4), 323-331.
- Noether, G. (1987). Sample size determination for some common nonparametric tests. *Journal of the American Statistical Association*, 82, 645-647.
- Norusis, M.J. (2005). *SPSS 13.0 guide to data analysis*. Upper Saddle River, NJ: Prentice Hall.
- Nunnally, J.C. & Bernstein, I. (1994). *Psychometric theory*. New York: McGraw-Hill.
- O’Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12), 2021-2040.
- Orlandi, E. (1991). The cost of security. *ACEA*, P.le Ostiense 2 - 00151, Rome, Italy, IEEE, 192-196.
- Otway, H., Maurer, D., & Thomas, K. (1978). Nuclear power: The question of public acceptance. *Futures*, 10, 109-118.
- Otway, H. & Haastrup, P. (1989, February). On the social acceptability of inherently safe technologies. *IEEE Transactions on Engineering Management*, 36(1), 57-60.
- Pallay, J. (2003, August). A brave new world. *Wall Street & Technology*, 31-32.
- Pedhazur, E.J. & Schmelkin, L.P. (1991). *Measure, design, and analysis: An integrated approach*. Hillsdale, NJ: Lawrence Erlbaum.
- Pett, M.A., Lackey, N.R., & Sullivan, J.J. (2003). *Making sense of factor analysis*. Thousand Oaks, CA: Sage.
- “Plant access with biometrics.” (2003, March). *Security*, 40(3), 52-53.
- Prabhakar, S., Pankanti, S., & Jain, A.K. (2003, March/April). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 33-42.
- “Prepare to be scanned; biometrics.” (2003, December 6). *The Economist*, 20.



- Putnam, R.G. (1987, Winter). Selling modernization within your company. *COMMLINE*, 13.
- Quantz, P. (1984, Fall). CIM planning: The future-factory foundation. *CIM Review*, 38.
- Ratha, N.K., Connell, J.H., & Bolle, R.M. (2001). Enhanced security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614-634.
- Reynolds, P. (2004, December). The keys to identity: As healthcare organizations strive for greater security, some are using a very personal approach in the form of biometrics. *Health Management Technology*, 25(12), 12-16.
- Richards, N. (2002). The critical importance of information security to financial institutions. *Business Credit*, 104(9), 35-36.
- Roberts, B. (2003, March). Are you ready for biometrics? *HRMagazine*, 48(3), 95-96.
- Roberts, G.K. & Pick, J.B. (2004). Technology factors in corporate adoption of mobile cell phones: A case study analysis. *Proceedings of the IEEE 37th Annual Hawaii International Conference on System Sciences*, 9(9), 90287-90296.
- Rogers, E.M. (2003). *Diffusion of innovations* (5th ed.). New York: The Free Press.
- Rummel, R.J. (1970). *Applied factor analysis*. Evanston, IL: Northwestern University Press.
- Rupley, S. (2002, July 1). A little bioprivacy, please. *PC Magazine*, 21(13), 24.
- Saccomano, A. (2003, September 9). Selling savings, not security. *Journal of Commerce*, 4(39), 22.
- Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzales-Marcos, A. (2000). Improving access control security using iris identification. *IEEE Symposia*, 56-59.
- Scheier, R. (2002, January 22). Biometrics: Improving but not perfect. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargt.com>.
- Schlaifer, R. (1959). *Probability and statistics for business decisions*. New York: McGraw-Hill.
- Schneier, B. (1999). Security in the real world: How to evaluate security technology. *Computer Security Journal*, 15(4), 1-14.
- Schneier, B. (2005, January 19). Schneier on security. Retrieved February 4, 2005 from <http://www.schneier.com/cgi-bin/mt-tb.cgi/99>.

- Schwartz, J. & Huddart, M. (2004, June 2). The promise of biometrics remains in doubt. *Airport Security Report*, 11(11), 1.
- Shore, J. (2004, November 1). Security summit. *Network World*. Retrieved August 25, 2005 from <http://www.networkworld.com/cgi-bin/mailbox/x.cgi>.
- Simon, H.A. (1955, February). A behavioral model of rational choice. *Quarterly Journal of Economics*, 69(1), 99-118.
- Simon, H.A. & Hayes, J.R. (1976). The understanding process: Problem isomorphs. *Cognitive Psychology*, 8, 165-190.
- Soo Hoo, K.J. (2000). How much is enough? A risk-management approach to computer security. *Working Paper*. Stanford University: Consortium for Research on Information Security and Policy (CRISP). Retrieved August 26, 2005 from <http://iis/db.stanford.edu/pubs/11900/soohoo.pdf>.
- Soto, C.A. (2003, May 5). Biometrics gets better but still needs some work: Iris authentication stands out as the most secure biometric technique in use today. *Government Computer News*, 22(10), 42-44.
- Stevens, J.P. (2002). *Applied multivariate statistics for the social sciences* (4th ed.). Mahwah, NJ: Lawrence Erlbaum.
- Strassmann, P. (2002, April 10). Problems with authentication. *SearchSecurity.com*. Retrieved February 4, 2005 from <http://www.searchsecuritytechtargt.com>.
- Straub, D.W. (1989, June). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169.
- Tabachnick, B.G. & Fidell, L.S. (2001). *Using multivariate statistics* (4th ed.). Needham Heights, MA: Allyn & Bacon.
- Teoh, A., Samad, S.A., & Hussain, A. (2003). An Internet based speech biometric verification system. *IEEE Symposia*, 47-51.
- Thorndike, R.M. (1978). *Correlational procedures for research*. New York: Gardner Press.
- Torantzky, L.G., Eveland, J.D., Boylan, M.G., Hetzner, W.A., Johnson, E.C., Reitman, D., & Schneider, J. (1983). *Innovation processes and their management: A conceptual, empirical and policy review of innovation process research*. Washington, D.C.: National Science Foundation.

- Tuggle, F.D. & Gerwin, D. (1980, June). An information processing model of organizational perception, strategy and choice. *Management Science*, 26(6), 575-592.
- Tversky, A. & Kahneman, D. (1974). Judgement under uncertainty: Heuristics and biases. *Science*, 185, 1124-1131.
- Ungson, G.R. & Braunstein, D.N. (1999). Introduction to decision making: An interdisciplinary inquiry. In *Decision Making: An Interdisciplinary Inquiry*. Boston: PWS.
- Van, J. (2004, October 4). IBM first major manufacturer to add biometric components to its computers. *Knight Ridder Tribune Business News*, 1.
- Verton, D. (2003, October 13). Scare tactics no longer guarantee security funding. *Computerworld*, 37(41), 10.
- Vijayan, J. (2005, April 11). Strategic security. *Computerworld*, 39(15), 48.
- Vijayan, J. (2004, August 9). Corporate America slow to adopt biometric technologies. *Computerworld*, 38(32), 1, 45.
- Vogel, L.H. (2004, December). 5 rules for effective IT investment planning. *Healthcare Financial Management*, 58(2), 92-95.
- Ward, J. (2004, April). How United Bankers' Bank ensures customer authentication. *Bank Systems + Technology*, 41(4), 41.
- Wikipedia. (2005). Retrieved June 4, 2005 from [http://en.wikipedia.org/wiki/Wikipedia:Wikiportal/Information\\_technology](http://en.wikipedia.org/wiki/Wikipedia:Wikiportal/Information_technology).
- Woodward, J.D., Orleans, N.M., & Higgins, P.T. (2003). *Biometrics*. New York: McGraw-Hill/Osborne.
- Yin, R.K. (2002). *Case study research: Design methods*. Thousand Oaks, CA: Sage.
- Young, S. (1972). The dynamics of measuring unchanged. In Haley, R.I. (Ed.), *Attitude Research in Transition*, Chicago: American Marketing Association, 61-82.
- Yun, J., & Ulrich, D.A. (2002). Estimating measurement validity: A tutorial. *Adapted Physical Activity Quarterly*, 19, 32-47.
- Zhang, D. (Ed.) (2002). *Biometric solutions for authentication in an e-world*. Boston: Kluwer Academic.